

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-225143

(43)Date of publication of application : 17.08.1999

(51)Int.Cl.

H04L 9/32
G06F 17/60
G06K 17/00
G07B 1/00
G07B 5/00
G07F 7/12
G09C 1/00



(21)Application number : 10-027074

(71)Applicant : FUJI XEROX CO LTD

(22)Date of filing : 09.02.1998

(72)Inventor : KIKO KENICHIROU

NAKAGAKI JUHEI

KIYOUJIMA HITOKI

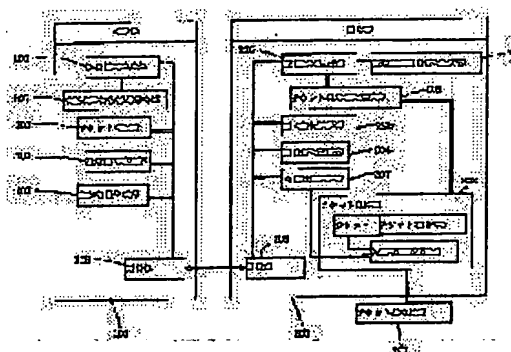
TANIGUCHI SHINICHIRO

(54) ELECTRONIC TICKET SYSTEM

(57)Abstract:

PROBLEM TO BE SOLVED: To prevent an internal state of a certificate device from being revised due to a ticket exhibited by mistake or illegally.

SOLUTION: An authentication information generating section 102 of an authentication device 100 generates authentication information and sends it to a certificate device 200. A ticket discrimination information generating section 203 of the certificate device 200 generates ticket discrimination information to indicate storage of a correct ticket from ticket utilization information and information in an internal state storage area. A certificate information generating section 206 connects ticket discrimination information to low-order bits of a bit stream of the authentication information to generate ticket certificate information. The ticket certificate information is sent to the authentication device 100 by a communication section 208. The authentication device 100 receiving the ticket certificate information conducts ticket discrimination processing and terminates the protocol when the ticket certificate information is incorrect or the ticket is not to be authenticated.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2000 Japanese Patent Office

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平 1 1 - 2 2 5 1 4 3

(43) 公開日 平成 1 1 年 (1 9 9 9) 8 月 1 7 日

(51) Int. Cl.	識別記号	庁内整理番号	F I	技術表示箇所
H04L 9/32			H04L 9/00	675 D
G06F 17/60			G06K 17/00	T
G06K 17/00				S
			G07B 1/00	A
G07B 1/00				B

審査請求 未請求 請求項の数 4 1 O L (全 2 9 頁) 最終頁に続く

(21) 出願番号 特願平 1 0 - 2 7 0 7 4
(22) 出願日 平成 1 0 年 (1 9 9 8) 2 月 9 日

(71) 出願人 0 0 0 . 0 0 5 4 9 6
富士ゼロックス株式会社
東京都港区赤坂二丁目 1 7 番 2 2 号
(72) 発明者 木子 健一郎
神奈川県足柄上郡中井町境 4 3 0 グリー
ンテクなかい 富士ゼロックス株式会社内
(72) 発明者 中垣 寿平
神奈川県足柄上郡中井町境 4 3 0 グリー
ンテクなかい 富士ゼロックス株式会社内
(72) 発明者 京嶋 仁樹
神奈川県足柄上郡中井町境 4 3 0 グリー
ンテクなかい 富士ゼロックス株式会社内
(74) 代理人 弁理士 澤田 俊夫

最終頁に続く

(54) 【発明の名称】 電子チケットシステム

(57) 【要約】

【課題】 誤って、または不正に提示されたチケットにより証明装置の内部状態が変更されないようにする。

【解決手段】 検証装置 1 0 0 の認証情報生成部 1 0 2 が、認証情報 C を生成し証明装置 2 0 0 に送る (S 3 1、S 3 2)。証明装置 2 0 0 のチケット判定情報生成部 2 0 3 は、正しいチケットを保持していることを示すためのチケット判定情報 M を、チケット利用情報および内部状態記憶領域の情報から生成する。証明情報生成部 2 0 6 は、認証情報 C のビット列の下位にチケット判定情報 M を連結し、チケット証明情報 T を生成する (S 3 3)。チケット証明情報 T は、通信部 2 0 8 により検証装置 1 0 0 に送られる (S 3 4)。T を受け取った検証装置 1 0 0 はチケット判定処理を行い、チケット証明情報が正しいものでない場合や、チケットが検証すべきでないもの場合には、プロトコルを終了する (S 3 5)。

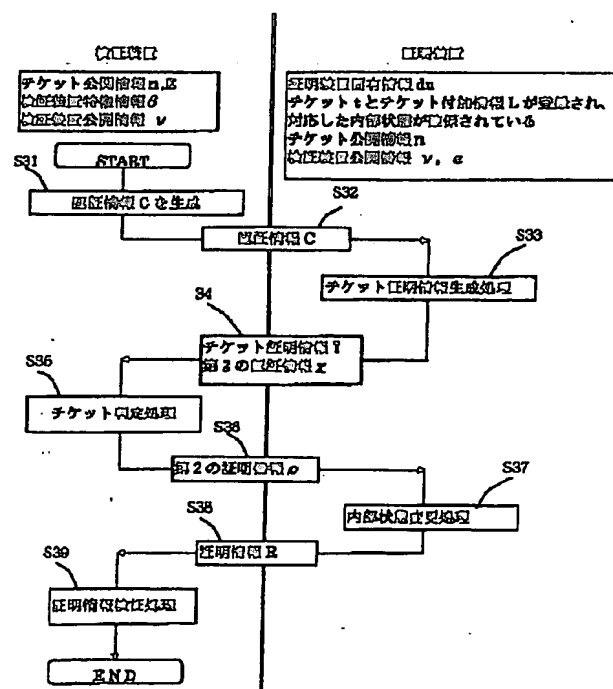


図 1 の処理全体のフローチャート

【特許請求の範囲】

【請求項 1】 証明装置と検証装置とを有し、上記証明装置が正当なチケットを所有していることを検証する電子チケットシステムであって、

上記証明装置は、

上記証明装置の固有情報を保持する証明装置固有情報保持手段と、

上記チケットを保持するチケット保持手段と、

上記チケットの権利内容または上記チケットの使用状態を表すチケット判定情報を生成するチケット判定情報生成部と、

少なくとも上記証明装置固有情報と上記チケットとからチケット秘密情報を生成し、上記チケット秘密情報を用いて証明情報を生成する証明情報生成手段とを有し、

上記検証装置は、

上記証明装置が提示する上記チケット判定情報に基づいて、検証処理を実行して良いかを判定するチケット判定手段と、

上記証明装置がチケット秘密情報を生成できたか否かを、上記証明情報に基づいて、検証する証明情報検証手段とを有することを特徴とする電子チケットシステム。

【請求項 2】 請求項 1 に記載の電子チケットシステムであって、

上記検証装置は、対話証明で用いられる認証情報を生成する認証情報生成手段を有し、

上記証明装置の証明情報生成手段は、上記検証装置が生成した認証情報を用いて上記証明情報を生成する電子チケットシステム。

【請求項 3】 請求項 2 に記載の電子チケットシステムであって、上記証明装置と上記検証装置とは通信手段を有し、上記証明装置は証明しようとするチケットのチケット判定情報を、上記検証装置に伝達する電子チケットシステム。

【請求項 4】 請求項 2 ないし 3 に記載の電子チケットシステムであって、

上記電子チケットシステムは、上記検証装置と上記証明装置とに加えて、チケット発行装置を有し、

上記チケット発行装置は、

発行するチケットの秘密の特徴情報である上記チケット秘密情報と対応するチケット公開情報を保持するチケット特徴情報保持手段と、

利用者が保持する上記証明装置の固有情報を保持するチケット発行用証明装置固有情報保持手段と、

上記チケット特徴情報保持手段に保持している上記チケット秘密情報と、上記チケット発行用証明装置固有情報保持手段に保持している上記証明装置固有情報とを用いて、デジタル情報であるチケットを作成するチケット発行手段とを有する電子チケットシステム。

【請求項 5】 請求項 2 ないし 4 の電子チケットシステムであって、上記証明装置の証明情報生成手段は、少な

くとも上記検証装置から送られた認証情報と、上記チケットと、上記チケット判定情報と、上記証明装置固有情報とより所定の方法で、上記証明情報の 1 つとして、上記チケット判定手段の判定に用いるチケット証明情報を計算する電子チケットシステム。

【請求項 6】 請求項 5 に記載の電子チケットシステムであって、上記証明装置はチケットの利用条件を定めたチケット利用情報を、チケットと対応させて上記チケット保持部に保持する電子チケットシステム。

【請求項 7】 請求項 5 に記載の電子チケットシステムであって、上記証明装置は、上記チケット判定情報を作成する際に、少なくとも上記チケット利用情報を用いる電子チケットシステム。

【請求項 8】 請求項 6 に記載の電子チケットシステムであって、上記証明装置は、可変な内部状態を保持する内部状態記憶領域と、上記内部状態の値を制御する内部状態制御手段とを備える電子チケットシステム。

【請求項 9】 請求項 8 に記載の電子チケットシステムであって、上記証明装置のチケット判定情報生成手段は、上記チケット判定情報を作成する際に、少なくとも上記証明装置の内部状態記憶領域の情報を用いる電子チケットシステム。

【請求項 10】 請求項 8 ないし 9 の電子チケットシステムであって、上記証明装置の内部状態記憶領域が保持する可変な内部状態のうちの、少なくとも一部は外部から書き換え不能である電子チケットシステム。

【請求項 11】 請求項 8 ないし 10 の電子チケットシステムであって、上記証明装置の証明情報生成手段は、少なくとも、上記チケットと、上記チケット利用情報と、上記証明装置固有情報とを用いて上記証明情報を計算する電子チケットシステム。

【請求項 12】 請求項 8 ないし 11 の電子チケットシステムであって、上記証明装置は、上記検証手段から送られた上記認証情報を保持する認証情報保持手段を有し、上記証明情報生成手段は、上記チケット判定情報生成手段により生成されたチケット判定情報を用いて、上記認証情報保持手段に保持されている認証情報を変更して上記証明情報の生成に利用する電子チケットシステム。

【請求項 13】 請求項 12 の電子チケットシステムであって、上記チケット判定情報生成手段が生成したチケット判定情報を M とし、上記認証情報を C とすると、上記証明装置の証明情報生成手段は、上記認証情報保持手段に保持されている認証情報 C を、C に M を接合したものに更新する電子チケットシステム。

【請求項 14】 請求項 12 ないし 13 の電子チケットシステムであって、上記証明装置の証明情報生成手段は、上記証明情報の 1 つとしてチケット証明情報を生成することが可能であり、上記チケット証明情報は、上記チケットと、上記チケット利用情報と、上記証明装置固

有情報とより所定の方法でチケット秘密情報を計算し、上記認証情報に対して、チケット秘密情報を用いた計算を施すことによって生成される電子チケットシステム。

【請求項15】 請求項14の電子チケットシステムであって、 p 、 q が素数であり、 $n=p \cdot q$ であり、 $DE \equiv 1 \pmod{(p-1)(q-1)}$ の関係が満たされるとき、上記チケット秘密情報が D であり、チケット公開情報が (n, E) であり、上記チケット利用情報が L であり、上記証明装置固有情報が秘密の値 du であり、 $f(du, L, n)$ を一方方向性関数として、チケットが $t=D-f(du, L, n)$ で与えられているとき、上記証明装置の証明情報生成手段は、上記認証情報 C （上記証明情報生成手段が変更した認証情報）に対して、 C の法 n での t による冪乗と、 C の法 n での一方方向性関数値 $f(du, L, n)$ による冪乗との法 n での積 $C^t C^{f(du, L, n)} \pmod{n}$ としてチケット証明情報を計算する電子チケットシステム。

【請求項16】 請求項14の電子チケットシステムであって、 p 、 q が素数であり、 $n=p \cdot q$ であり、 $DE \equiv 1 \pmod{(p-1)(q-1)}$ の関係が満たされるとき、上記チケット秘密情報が D であり、チケット公開情報が (n, E) であり、上記チケット利用情報が L であり、上記証明装置固有情報が秘密の値 du であり、 $f(du, L, n)$ を一方方向性関数として、上記チケットが $t=D-f(du, L, n)$ で与えられているとき、上記証明装置は、あらかじめ $t+f(du, L, n)=D$ を計算し、その値を用いて、上記認証情報 C （上記証明情報生成手段が変更した認証情報）に対して、 $T=C^D \pmod{n}$ としてチケット証明情報 T を計算する電子チケットシステム。

【請求項17】 請求項14の電子チケットシステムであって、 g が離散対数問題が困難な群の原始根であり、 p が素数であり、整数 x に対して $y=g^x \pmod{p}$ が成り立つとき、上記チケット秘密情報が x であり、チケット公開情報が (y, p, g) であり、上記チケット利用情報が L であり、上記証明装置固有情報が秘密の値 du であり、 $f(du, L, y)$ を一方方向性関数として、上記チケットが $t=x-f(du, L, y)$ で与えられているとき、上記証明装置は、上記認証情報 C （上記証明情報生成手段が変更した認証情報）に対して、上記チケット判定情報 T を C の法 p での t による冪乗と、 C の法 p での一方方向性関数値 $f(du, L, y)$ を指数とする冪乗との法 p での積 $C^t C^{f(du, L, y)} \pmod{p}$ として上記証明情報を計算する電子チケットシステム。

【請求項18】 請求項14の電子チケットシステムであって、 g が離散対数問題が困難な群の原始根であり、 p が素数であり、整数 x に対して $y=g^x \pmod{p}$ が成り立つとき、上記チケット秘密情報が x であり、チケット公開情報が (y, p, g) であり、上記チケット利用情報が L であり、上記証明装置固有情報が秘密の値 d

u であり、 $f(du, L, y)$ を一方方向性関数として、上記チケットが $t=x-f(du, L, y)$ で与えられているとき、上記証明装置は、あらかじめ $t+f(du, L, y)=x$ を計算し、上記認証情報 C に対して（上記証明情報生成手段が変更した認証情報）チケット判定情報 T を計算する際に、 $C^t \pmod{p}$ の値を用いる電子チケットシステム。

【請求項19】 請求項14ないし18の電子チケットシステムであって、上記検証装置の証明情報検証手段は、上記認証情報生成手段が作成した認証情報と、上記証明装置から送られたチケット証明情報と、上記チケット公開情報とより、上記チケット証明情報の正当性を検証し、上記チケット証明情報が正しい場合は、上記チケット証明情報に埋め込まれたチケット判定情報を導出する電子チケットシステム。

【請求項20】 請求項19の電子チケットシステムであって、上記認証情報が C であり、上記チケット証明情報が T であり、上記チケット公開情報 (n, E) であり、あるビット列 M がある場合に、上記検証装置の証明情報検証手段は、上記チケット証明情報 T を法 n で E でべき乗したものを C と M とを接合したビット列と比較し、 $T^E \pmod{n}=C||M$ （記号 $||$ はビット列の接合）となっていれば、上記チケット証明情報は正しいと判定し、上記チケット証明情報が正しい場合は M を上記チケット判定情報として導出する電子チケットシステム。

【請求項21】 請求項19の電子チケットシステムであって、上記認証情報が C であり、上記チケット証明情報が T であり、上記チケット公開情報が (p, g, y) である場合に、上記検証装置の証明情報検証手段は、自身が発生させた乱数を r とすると、あるビット列 M があつて、 $T/y^r \pmod{p}=(C||M)$ （記号 $||$ はビット列の接合）となっていれば、上記チケット証明情報は正しいと判定し、上記チケット証明情報が正しい場合は M をチケット判定情報として導出する電子チケットシステム。

【請求項22】 請求項8ないし21の電子チケットシステムであって、

上記証明装置は、上記検証装置を認証するための第2の認証情報を生成する、第2の認証情報生成手段と、上記検証装置が生成する第2の証明情報を検証するための、第2の証明情報検証手段とを有し、

上記第2の証明情報検証手段は、上記第2の認証情報と、上記第2の証明情報と、チケット公開情報とより上記第2の証明情報が正しいかどうかを検証し、

上記第2の証明情報が正しい場合、上記内部状態制御手段は、上記証明装置の内部状態を変更する電子チケットシステム。

【請求項23】 請求項22の電子チケットシステムであって、上記検証装置の証明情報検証手段は、上記チケ

ット判定手段による判定の結果をもとにして、上記第 2 の証明情報を生成するか否かを決定する電子チケットシステム。

【請求項 2 4】 請求項 2 2 の電子チケットシステムであって、

上記証明装置は、チケットのカウンタとして機能する内部状態をチケットと関連づけ、外部から書き換え不能な形で、内部状態記憶領域に保持し、

上記検証装置の証明情報検証手段は、上記証明装置から送られたチケット判定情報に含まれる内部状態のカウンタの値が、所定の値であるときには、対応するチケットが無効であるものと判断する電子チケットシステム。

【請求項 2 5】 請求項 2 2 ないし 2 4 の電子チケットシステムであって、 p' 、 q' が素数であり、 $v = p' \cdot q'$ であり、 $\delta \varepsilon \equiv 1 \pmod{(p' - 1)(q' - 1)}$ の関係が満たされるときに、上記証明装置の第 2 の証明情報検証手段は、上記第 2 の認証情報 x と上記第 2 の証明情報 ρ が

【数 1】

$$x = \rho^{\delta} \pmod{v}$$

を満たす場合に上記第 2 の証明情報が正しいと判定する電子チケットシステム。

【請求項 2 6】 請求項 2 2 ないし 2 4 の電子チケットシステムであって、 g が離散対数問題が困難な群の原始

$$x \parallel \mu = \rho^{\delta} \pmod{v} \quad (\text{記号 } \parallel \text{ はビット列の接合})$$

を満たすときに、上記第 2 の証明情報が正しいと判定し、 μ を上記第 2 の証明情報に埋め込まれた情報として導出する電子チケットシステム。

【請求項 3 0】 請求項 2 7 の電子チケットシステムであって、上記証明装置の内部状態制御手段は、上記第 2 の証明情報から導出された情報にもとづいて上記内部状態記憶領域に保持された内部状態を変更する電子チケットシステム。

【請求項 3 1】 請求項 3 0 の電子チケットシステムであって、上記証明装置の上記第 2 の証明情報検証手段は、上記検証装置より送られた内部状態変更を許可する情報と、内部状態とに基づいて、上記証明情報を正しく生成するか否かを判定する電子チケットシステム。

【請求項 3 2】 請求項 2 2 ないし 3 1 の電子チケットシステムであって、上記検証装置は、上記検証装置の特権を表す秘密情報である、検証装置特権情報を保持する検証装置特権情報保持部と、上記第 2 の証明情報を生成する第 2 の証明情報生成部を有し、

上記第 2 の証明情報生成部は、上記第 2 の認証情報と上記検証装置特権情報とより第 2 の証明情報を生成する電子チケットシステム。

【請求項 3 3】 請求項 3 2 の電子チケットシステムであって、上記検証装置特権情報を δ とし、対応する公開情報を (v, ε) とするとき、上記検証装置の第 2 の証明情報生成部は、上記第 2 の認証情報 x より上記第 2 の

根であり、 p が素数であり、整数 ε に対して

【数 2】

$$\eta = g^{\varepsilon} \pmod{p}$$

が成り立つときに、証明装置の第 2 の認証情報生成手段は、乱数 r' と上記第 2 の認証情報 $x = g^{r'}$ を生成し、上記第 2 の証明情報検証手段は上記第 2 の証明情報 ρ について、 $\rho / \eta \pmod{p} = x$ が満たされた場合に上記第 2 の証明情報が正しいと判定する電子チケットシステム。

【請求項 2 7】 請求項 2 2 の電子チケットシステムであって、上記証明装置の第 2 の証明情報検証手段は、上記第 2 の証明情報が正しい場合は、上記第 2 の証明情報に埋め込まれた情報を導出する電子チケットシステム。

【請求項 2 8】 請求項 2 7 の電子チケットシステムであって、上記証明装置の第 2 の証明情報検証手段は、上記第 2 の証明情報から導出された情報を、上記内部情報の変更を許可するための情報として利用する電子チケットシステム。

【請求項 2 9】 請求項 2 7 ないし 2 8 の電子チケット

システムであって、チケット公開情報は v および ε を含んでおり、上記証明装置の第 2 の証明情報検証手段は、上記第 2 の認証情報 x と上記第 2 の証明情報 ρ とが、あるビット列 μ に対して、

【数 3】

証明情報 ρ を

【数 4】

$$\rho = x^{\delta} \pmod{v}$$

として生成する電子チケットシステム。

【請求項 3 4】 請求項 3 2 の電子チケットシステムであって、上記検証装置特権情報を ε 、対応する公開情報を (p, g, η) とし、

【数 5】

$$\eta = g^{\varepsilon} \pmod{p}$$

の関係が満たされるとき、上記検証装置の第 2 の証明情報生成部は上記第 2 の認証情報 x に対して、

【数 6】

$$x^{\varepsilon} \pmod{p}$$

の値を用いて上記第 2 の証明情報 ρ を生成する電子チケットシステム。

【請求項 3 5】 請求項 3 2 ないし 3 4 の電子チケットシステムであって、上記検証装置は上記第 2 の認証情報を保持する、第 2 の認証情報保持部を有し、上記検証装置の第 2 の証明情報生成部は、上記検証装置特権情報を用いた計算を施す際に、証明装置の内部状態の変更を許可する情報と、上記第 2 の認証情報より上記第 2 の証明情報を計算する電子チケットシステム。

【請求項 3 6】 請求項 3 2 ないし 3 4 の電子チケットシステムであって、上記検証装置の第 2 の証明情報生成部は、上記検証装置特権情報を用いた計算を施す前に、

上記証明装置の内部状態の変更を許可する情報を用いて、上記第 2 の認証情報保持部に保持された上記第 2 の認証情報を更新する電子チケットシステム。

【請求項 3 7】 請求項 3 6 の電子チケットシステムであって、上記検証装置の第 2 の証明情報生成部は、上記証明装置の内部状態の変更を許可する情報を μ とし、上記第 2 の認証情報を χ とすると、上記第 2 の認証情報保持部に保持された第 2 の認証情報を χ に μ を接合したものに更新する電子チケットシステム。

【請求項 3 8】 請求項 1 ないし 3 7 に記載の電子チケットシステムであって、少なくとも、上記証明装置が、内部のデータ及び処理手続きを外部から観測することを困難ならしめる防御手段中に保持されている電子チケットシステム。

【請求項 3 9】 請求項 1 ないし 3 7 に記載の電子チケットシステムであって、少なくとも、上記証明装置が、IC カードなどの携帯可能な小型演算装置として構成されている電子チケットシステム。

【請求項 4 0】 証明装置と検証装置とを有し、上記証明装置が正当なチケットを所有していることを検証する電子チケットシステムであって、

上記証明装置は、

上記証明装置の固有情報を保持する証明装置固有情報保持手段と、

上記チケットを保持するチケット保持手段と、

上記チケットの権利内容または上記チケットの使用状態を表すチケット判定情報を生成するチケット判定情報生成部と、

少なくとも上記証明装置固有情報と上記チケットとから証明情報を生成する証明情報生成手段とを有し、

上記検証装置は、

上記証明装置が提示する上記チケット判定情報に基づいて、検証処理を実行して良いかを判定するチケット判定手段と、

上記証明装置が上記証明装置固有情報と上記チケットから上記証明情報を生成できたか否かを検証する証明情報検証手段とを有することを特徴とする電子チケットシステム。

【請求項 4 1】 検証装置と電子チケットを保持する認証装置との間で相互認証を行ないながら検証装置側で所定のサービスを実行し、認証装置側で内部状態を変更する電子チケット利用方法において、

上記証明装置が、上記電子チケットの権利内容または上記電子チケットの使用状態を表すチケット判定情報を上記検証装置に提示するステップと、

上記検証装置が、提示された上記チケット判定情報に基づいて、検証処理を実行して良いかを判定するステップとを有することを特徴とする電子チケット利用方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、チケットやカードを電子的に作成し利用する技術に関する。

【0002】

【背景の技術】 【従来の技術】 近年、乗車券、入場券、指定券、予約券、回数券、定期券、プリペイドカード、ポイントカード、などの一般的なチケットを、電子チケットとして発行する試みが行われている。

【0003】 このような電子チケットは、発行者が、利用者に与えた権利を特定でき、正しいチケットであることを検証できるという機能を持つ。電子情報は、作成が容易であり、通信回線を通して送信できるという特長を持つが、完全なコピーを簡単に作れるので、電子チケットの実現には、偽造と複製による不正利用への対策が不可欠である。電子署名により偽造の防止は可能だが、複製の防止は困難であり、複製による不正利用を防止することが、電子チケットの実現にあたっての最大の課題となっていた。

【0004】 この問題に対する、解決策として、従来、チケットの利用時に正当な利用者か確認する第 1 の従来技術、発行者以外の者にチケットを複写する機会を与えない第 2 の従来技術、検証時の通信を公開できるように第 2 の従来技術を修正した第 3 の従来技術の、3 つの方法が提案されてきた。

【0005】 第 1 の従来技術は、チケットの利用時に利用者が、正当な利用者かどうかを確認する方法であり、利用者は、チケットを利用する時に、チケットとともに、自分が利用者特定情報に適合する正当な利用者であることを示す。利用者特定情報に適合していれば、対応する権利の行使が認められる。確認のために必要な情報（利用者特定情報）と、与えた権利とを対応づける情報がチケットとして発行され、利用者が記録管理する。発行者以外の者が勝手にチケットを偽造できないようにするためには、発行者がチケットに電子署名を施す。電子署名のないチケットは、偽造されたものと判断される。利用者特定情報には、身元、顔写真などの身体的特徴、パスワードなどの知識の所有などが利用できる。

【0006】 しかしながら、この方法では、利用する利用者特定情報に応じて、いくつかの問題点が生ずる。

【0007】 例えば、利用者特定情報に利用者の身元を利用する方法では、発行時と検証時に利用者の身元が明らかになり、匿名性が失われてしまう。また、通信回線を利用した遠隔的な環境で身分を安全に証明する方法は実現されていないので、このような環境では正当な権利を持たないものが、不当にチケットを利用することを防止することができない。

【0008】 利用者特定情報にパスワードを利用すれば、匿名性の問題は軽減されるが、パスワードを記憶する負荷を利用者に与える。また、利用者が故意にパスワードを漏洩させることを防止できないので、不正利用の危険が増してしまうという問題点もある。

【0009】第2の従来技術は、例えば特開平8-147500号公報に示されるようなものであり、発行者以外の者にチケットを複写する機会を与えない方法である。この方法では、利用者が保持管理しているチケットを複写できないようにする機構と、発行時や検証時の通信からチケットが漏洩しない機構の両方を必要とする。

【0010】しかしながら、この方法では

(1) 発行者以外の者はチケットを複写できないので、チケットの正当性を第三者に証明することが困難になる、(2) チケットの発行時と検証時の通信の内容も機密に行うので、チケットの発行時と検証時にプライバシーなどの利用者の権利が侵害されていないことを証明できない、といった問題点が生ずる。

【0011】第3の従来技術は、例えば特公平6-52518号公報に示されるようなものであり、検証時の通信を公開できるように、第2の従来技術を修正した方法である。この方法では、第2の従来技術と同様に、チケットを秘密情報として利用者の所持する装置(証明装置)に複写できないように記録するが、検証の方法が異なっている。まず、検証を行う検証装置は、証明装置に乱数などの繰り返し利用されない値(チャレンジ)を送る。証明装置は、チケットである秘密情報を利用した演算をチャレンジに対して施して、得られた値(レスポンス)を検証装置に送り返す。検証装置は、秘密情報とチャレンジを利用してレスポンスが演算されたことを確認することで、利用者の正当性を認証する。レスポンスから逆に秘密情報を求めることを計算量的に困難とすることで、チャレンジとレスポンスを秘密通信とする必要がなくなる。

【0012】この方法は、認証のために利用されるものであり、正当なチケットを保持しているか否か以外に情報を伝達しない。このため、有効期限などを示すことができず、単純なチケットしか表現できない。また、チケットを証明装置に送信する方法が、第2の従来技術と同様に機密通信で行う必要があり、不当に利用者の情報を開示して利用者の権利を侵害していないことを証明できないという問題があった。

【0013】このように、従来の技術はいずれも、チケットに必要な不正利用を防止する機能を実現するために、第三者に対するチケットの内容証明の機能や利用者の匿名性を犠牲にしている点に、問題があった。

【0014】[関連技術] これらの問題を解決する関連技術として、特願平9-188064号(平成9年7月14日、未公開)に示す方法が提案されている。

【0015】この関連技術の一般的な認証プロトコルを図1に示す。このプロトコルは、双方向の認証を行うプロトコルであり、双方が認証情報(発生した乱数)に対する署名を確認することによって、お互いの正当性を認証する。相互の認証情報(乱数)の一部にメッセージ

(m 、 μ)を含ませることにより、情報の安全な伝達を

可能にしている。

【0016】図1を参照して関連技術のプロトコルについて説明する。図1において、はじめに、検証装置が乱数に基づいて認証情報Cを生成し(S11)、この認証情報Cを証明装置に対して送る(S12)。他方、証明装置は乱数に基づいて別の認証情報 x を生成し、認証情報 x を検証装置に送る(S13、S14)。証明装置にはチケットに対応して、外部からは操作不能な内部状態があり、検証装置からの応答情報によってのみ書き換えが可能となっている。検証装置は x の一部に、内部状態の変更を許可する情報(μ)を含ませた応答情報を作成し、検証装置が署名して証明装置に送る(S15、S16)。証明装置は応答情報 ρ の署名を確認することにより、送信者が正当な検証装置であることを確認し、それをもって内部状態変更の情報 μ の正しさを確認する(S17)。 ρ が正しい場合にのみ、証明装置の内部状態が μ の内容にしたがって変更される(S18)。証明装置は、正当に作成されたチケット t と証明装置固有情報 d から、Dを復元することが可能であり(S19)、最後に証明情報RにDによる署名を施して、検証装置に送り(S20、S21)、検証装置はその署名を確認することにより、定められたサービスを提供する(S22、S23)。

【0017】この方法によれば、チケットの検証情報は公開であるため第3者にもチケットの検証が可能であり、利用者はチケットの検証時に利用者を特定する情報を提示する必要が無いことから、匿名性も守られている。

【0018】また、検証装置と証明装置がそれぞれの秘密情報と公開情報を持ち合い、相互の認証をすることにより、証明装置・検証装置の偽造の問題を解決している。さらに、この証明に用いる認証情報の一部に、伝達したい情報を埋め込むことにより、検証装置・証明装置相互の情報伝達をも可能にしておき、チケットの内容を証明することができる。

【0019】このように、この関連技術の方法を使うと、電子チケットの基本的な機能をすべて満たした安全な電子チケットを実現することができ、上記の問題をすべて解決することが可能である。

【0020】ところで、先の関連技術では、検証装置がチケットを特定する情報を証明装置に送ることにより、検証装置が検証しようとするチケットが証明装置の中で一意に定まることを前提としている。しかし、実際には、その検証装置で検証可能なチケットが証明装置内に複数存在することも考えられる。たとえば、鉄道の乗車券のようなものを考えた場合、その駅から有効な回数券や定期券など複数のチケットが証明装置の中に存在することがありうる。そのような場合、証明装置では、どのチケットを利用者が利用しようとしているのか判断することができない。そこで、こういった場合には、利用者

があらかじめ利用するチケットを選択する必要が生ずる。

【0021】そして、このような場面において、先の関連技術を適用すると、チケットに対応する内部状態の変更を許可する応答情報が、選択・提示されたチケットの内容を確認することなしに作成され、送られてしまうという問題が生ずる。

【0022】これは、例えば、利用者が誤ったチケットを選択してしまった場合に、意図しないチケットの内部状態が変更されてしまうことを意味している。

【0023】また、鉄道の切符に適用する場合を考えると、内部状態として、入場の記録を残しておき、出場時に入場の記録を確認することにより、キセルのような不正行為を防止することが考えられる。

【0024】ここで、入場の情報として、単に入場したという事実のみを、チケットに対応する内部状態に残すような場合を考える。このような場合、内部状態の変更許可情報、具体的には入場情報を、提示されたチケットの内容を確認すること無く証明装置に送ってしまうと、本来その駅では入場できないチケットに対しても、入場したという事実を残すことが可能になる。実際には正当でないチケットでの入場はできないが、入場を拒否された段階で、内部状態が書き換えられたチケットを保持している証明装置を手に入れることができるとすると、実際に入場した駅よりも目的駅に近い駅からのチケットに対する入場記録を偽造すれば、出場時に偽造した入場記録を持つチケットを提示することで、キセル行為が可能になってしまう。

【0025】このように、利用者が、証明しようとするチケットを自ら選択するような場合には、検証装置は、内部状態を変更する許可情報を作成する前に、提示されたチケットがその検証装置で正当に検証可能であることを確認する必要がある。

【0026】しかし、先の関連技術においては、このような確認が成されないため、利用者が誤って意図しないチケットに対応する内部状態を書き換えてしまったり、内部状態を書き換えることによる不正が可能であったりするという問題点があった。

【0027】

【発明が解決しようとする課題】本発明では、上記の問題を解決するために、検証装置が検証可能なチケットのみを検証し、検証することが正しくないチケットに対しては、内部状態の変更を許可する情報を生成しないような電子チケットシステムを実現することを目的とする。

【0028】

【課題を解決するための手段】上記の課題を解決するため、本発明に係わる電子チケットシステムは、チケット検証装置と証明装置からなり、チケット検証装置は、検証するチケットが検証装置で検証可能かどうかを、証明装置が提示するチケット判定情報に基づいて判定するチ

ケット判定手段と、証明装置がチケット秘密情報を算出できたか否かを検証する対話検証手段を有し、証明装置は、証明装置固有情報保持手段と、チケット保持手段と、少なくとも証明装置固有情報とチケットからチケット秘密情報に関する知識の証明を行える対話証明手段とを有している。

【0029】この構成においては、検証装置が、チケット判定情報に基づいて、証明装置内のチケットの適合性をチェックでき、正しいチケットが提示されたときのみに証明装置の内部状態を変更するようになっている。

【0030】

【発明の実施の態様】以下、本発明を詳細に説明する。

【0031】【実施例1】図2に本発明の実施例1の電子チケットシステムの構成図を示す。図2において、本実施例に示す電子チケットシステムは、検証装置（検証器ともいう）100と証明装置（証明器ともいう）200とチケット指定装置300とからなる。

【0032】検証装置100は、検証するチケットの正当性を判定するチケット判定部101と、認証情報生成部102と、証明情報生成部103と、証明情報検証部104と、検証装置特権情報保持部105と、通信部106とを含んで構成される。

【0033】一方、証明装置200は、証明装置固有情報保持部201と、チケット保持部202と、チケット判定情報生成部203と、認証情報生成部204と、証明情報検証部205と、証明情報生成部206と、内部状態制御部207と、通信部208とを含んで構成される。なお検証装置100の証明情報生成部103、認証装置200の証明情報生成部206は、それぞれ認証装置200、検証装置100から送られてくる認証情報を保持する記憶部を具備している。

【0034】また、チケット保持部202にはチケットと、各チケットに対応するチケット利用情報とが保存される。また、チケット保持部202には各チケットに対応する内部状態記憶領域が確保される。

【0035】ここでは、証明装置200は、内部のデータや処理手続きを外部から観測することが困難なICカードのような媒体により構成される。

【0036】また、この実施例では以下のように、チケットtが発行される。

【0037】

【表1】

チケット： $t = D - F(n, L, du)$

D：チケット秘密鍵

du：証明装置固有の秘密情報

n：チケット法数

F：非衝突性一方関数

L：チケット利用情報

ただし、

$ED \equiv 1 \pmod n$

ここでE: チケット公開鍵

である。チケット秘密情報がDであり、チケット公開情報は、E, n, Lである。Fは一般のハッシュ関数によって実現可能である。また、チケット利用情報Lには、そのチケットを利用する条件、例えば有効期限や、サービスを受けられる場所などの情報が入る。

【0038】本発明の認証プロトコルの概略を図3に示す。はじめに利用者は、これから利用するチケットをチケット指定装置300により証明装置200に指定した上で、検証装置100と証明装置200との間で認証プロトコルが開始される。

【0039】図3において、認証プロトコルでは、まず検証装置100の認証情報生成部102が、認証情報として乱数Cを生成し証明装置200に送る(S31、S32)。

【0040】認証情報を受け取った証明装置200は、チケット証明情報生成処理を実行する(S33)。

【0041】チケット証明情報生成処理(S33)のフローチャートを図4に示す。図4において、まず証明装置200の証明情報生成部206は、署名に用いる秘密鍵Dを、チケットtとチケット利用情報Lおよび証明装置固有情報保持部201に保存されている証明装置固有情報duから、以下の計算により算出する(S41)。

【0042】

【数7】

$$\begin{aligned} & t + F(n, L, du) \\ &= D - F(n, L, du) + F(n, L, du) \\ &= D \end{aligned}$$

次に、チケット判定情報生成部203は、正しいチケットを保持していることを示すためのチケット判定情報Mを、チケット保持部202のチケット利用情報および内部状態記憶領域の情報から生成する(S42)。証明情報生成部206は、認証情報Cのビット列の下位にチケット判定情報Mを連結し(S43)、チケット証明情報Tを、

【0043】

【数8】 $T = (C || M)^e \bmod n$

の計算により生成する(S44、なお記号||はビット列に連結することを示す)。なお上記の計算以外にも、

【0044】

【数9】

$T = (C || M)^e (C || M)^{f(n, L, du)} \bmod n$ により、証明情報Tを計算しても良い。

【0045】また、認証情報生成部204は、乱数xを生成し第2の認証情報とする(S44)。

【0046】チケット証明情報Tと第2の認証情報xは、通信部208により検証装置100に送られる(S34)。この署名をするのは、チケット証明情報が正しいものであり、証明装置・チケット判定情報が偽造されていないことを保証するためである。

【0047】Tとxを受け取った検証装置100はチケット判定処理(図3のS35)を行う。

【0048】チケット判定処理(図3のS35)のフローチャートを図5に示す。図5において、検証装置100の証明情報検証部104は、送られたチケット証明情報Tと証明情報検証部が保持しているチケット公開情報Eから、

【0049】

【数10】 $T^d \bmod n$

の値を計算し、そのビット列のうち、連結された上位ビットの部分が、認証情報Cと一致するかどうかを確認する(S51)。一致した場合には、さらにチケット判定情報Mを抽出する(S52)。次に、チケット判定部101は、Mの内容をもとにチケット及びチケットに関連付けられた内部状態がこの検証装置で検証して良いものかどうかを判定する(S53)。判定の結果、このチケットを検証して良い場合には、証明情報生成部103は、証明装置200の内部状態の変更を指示する情報μを作成して、xの下位に連結する(S54、S55)。さらに、この値に対して、検証装置の特権を表す秘密情報δを用いて署名をした値ρを作成する(S56)。作成されたρは、通信部106により証明装置200へと送られる(S36)。

【0050】一方、チケット証明情報が正しいものでない場合や、チケットが検証すべきでないものの場合には、プロトコルを終了する(S57)。

【0051】次にρを受け取った証明装置は内部状態変更処理(図3のS37)を行う。

【0052】内部状態変更処理(図3のS37)のフローチャートを図6に示す。図6において、証明装置200の証明情報検証部205は、送られた第2の証明情報ρに対して、自身が保持している検証装置100の特権を確認する公開情報εを用いて

【0053】

【数11】

$$\rho^e \bmod n$$

を計算し、そのビット列のうち、上位の部分が、第2の認証情報xと一致するかどうかを確認する(S61)。確認の結果、正しくないことが判明した場合には場合には、プロトコルを終了する(S62)。正しいものであることが確認できた場合には、連結されたμを抽出する(S63)。内部状態制御部207は、μの内容に応じて証明装置200の内部状態を変更し、その結果をM'とする(S64、S65)。証明情報生成部206はM'の値を認証情報Cのビット列に連結した上で、

【0054】

【数12】 $R = (C || M')^e \bmod n$

の計算により、証明情報Rを生成する(S66、S67)。Rは通信部208により検証装置100に送られる(S38)。

【0055】Rを受け取った検証装置100は、証明情報検証処理（図3のS39）を行う。

【0056】証明情報検証処理（図3のS39）のフローチャートを図7に示す。図7において、検証装置100の証明情報検証部104は保持しているチケット公開情報Eを用いて、

【0057】

【数13】 $R' \bmod n$

の値を計算し、その結果連結されたM'を除いた上位のビット列が、最初に検証装置100が生成した認証情報Cと一致することを確認する（S71）。確認できた場合は、さらに内部状態の変更結果を表す情報M'の内容が、第2の証明情報ρとして送った、内部状態変更を許可する情報μと一致するかどうかを確認し（S72、S73、S74）、確認ができた場合には、定められたサービスを提供する（S75）。いずれかの確認に失敗した場合には、プロトコルが終了し、サービスの提供は行われない（S71、S74、S76）。

【0058】【実施例2】本発明の実施例2は、実施例1を鉄道の切符の乗車券として実現した場合である。ここでは特に、乗車券の入場時のプロトコルを説明する。

【0059】本発明の実施例の構成やチケットの生成方法は実施例1と同様であるが、検証装置100は具体的には自動改札機であり、証明装置200はチケットを保持することができる、ICカードのようなトークンである。そして、入場、出場ともに自動改札による検証が行われ、内部状態には入場や出場に対応した記憶領域が確保されるものとする。

【0060】以下では、横浜～成田空港1997年7月18日の乗車券の例で説明する。なお、適宜、図3の対応するステップ等を指摘する。

【0061】チケットのチケット利用情報Lは、図9のようになる。チケットは証明装置200に登録されており、対応した内部状態記憶領域が確保されている。入場前の内部状態を図8に示す。ここで、これから使用するチケットは、チケットIDが00005に示すものである。

【0062】まず、入場時の認証について説明する。はじめに検証装置100は認証情報Cとともに、入場であることをあらわす情報を証明装置200に送る（S32）。

【0063】証明装置200は、チケット判定情報Mを生成する。Mの内容を図10に示す。チケット判定情報Mには、図に示すように、チケット利用情報に含まれる内容と、使用状態を示すための、内部状態の入場・出場記録の内容が含まれている。証明情報生成部206は、MをCに連結し、チケット秘密鍵Dによる署名を施して、チケット証明情報Tとして、生成した第2の認証情報χとともに検証装置100に送る（S34）。

【0064】検証装置100は、チケット証明情報を検

証し、さらにチケット判定情報Mの内容を確認する。ここでは、入場駅が横浜駅で、有効期限内であり、未使用のチケットであることから、ここでの認証をしてよいチケットであると判定される（S35）。

【0065】そこで、証明装置200の内部状態を変更するための情報μが作成される。μの内容を図11に示す。μには、入場駅名と時間が記録される。証明情報生成部103は、こうして生成したμを第2の認証情報χに連結し、検証装置100の特権情報δによる署名を施した値ρを生成して、証明装置200へ送る（S36）。

【0066】証明装置200の証明情報検証部205は、送られたρの値が、認証情報χと一致するかどうかを確認する。正しいものであることが確認できた場合には、内部状態制御部207がμの内容に応じて、証明装置200の内部状態を変更する（S37）。変更後の内部状態の様子を図12に示す。入場の駅と時間が記録されたことがわかる。次に、内部状態制御部207はこの内部状態の変更、すなわち入場記録の内容をM'とする。実施例1と同様に、証明情報生成部206は、M'の値を認証情報のビット列に連結して、チケット秘密情報による署名を施した値Rを生成して、証明情報Rとして検証装置100に送る（S38）。

【0067】検証装置100は証明情報Rの値を検証し、その値が認証情報Cと一致した場合には、さらに内部状態を変更した結果M'を確認する。M'がμで指定したものと対応していれば、正しく内部状態が変更されたものと判断し、改札機のゲートを開ける。

【0068】次に、出場時の認証を説明する。出場時の認証は、入場時とほぼ同様であるが、相互に伝えられるメッセージの内容が異なる。

【0069】はじめに検証装置100は認証情報Cとともに、出場であることをあらわす情報を証明装置に送る（S32）。

【0070】証明装置200のチケット判定情報生成部203はチケット判定情報Mを生成する。出場時のMの内容を図13に示す。証明情報生成部206は、MをCに連結し、チケット秘密鍵Dによる署名を施し、チケット証明情報Tとする。そして、証明情報Tと、認証情報生成部生成した第2の認証情報χが検証装置に送られる（S34）。

【0071】検証装置100の証明情報検証部104は、チケット証明情報を検証する。チケットの検証結果が正しい場合には、チケット判定部101が、チケット判定情報Mの内容を確認する。ここでは、入場駅が横浜駅で有効な入場記録であり、出場の有効期間内であることから、ここでの出場の認証が可能なチケットであると判定される（S35）。

【0072】次に、証明情報生成部103は証明装置200の内部状態を変更するための情報μを作成する。μ

の内容を図 14 に示す。μ には、出場駅名と出場時間が記録される。証明情報生成部 103 は、さらに、生成された μ を x に連結し、検証装置の特権情報 δ による署名を施した値 ρ を生成する。ρ は証明装置 200 へと送られる (S36)。

【0073】証明装置 200 の証明情報検証部 205 は、送られた ρ の値が、認証情報 x と一致するかどうかを確認する。正しいことが確認できた場合には、内部状態制御部 207 が μ の内容に応じて、証明装置 200 の内部状態を変更し、この変更結果、すなわち出場記録を M' とする。変更後の内部状態の様子を図 15 に示す。出場駅と時間が記録される。証明情報生成部 206 は、出場記録 M' を認証情報 C のビット列に連結して、チケット秘密情報による署名を施した証明情報 R を生成し、検証装置 100 に送る (S38)。

【0074】検証装置 200 の証明情報検証部 104 は R の値を検証し、その値が認証情報 C と一致した場合には、さらに内部状態を変更した結果 M' を確認する。M' が μ の値で指定したものと対応していれば、正しく内部状態が変更されたものと判断し、出場を許可して、改札機のゲートを開ける (S39)。

【0075】【実施例 3】実施例 3 では、回数券のような形態を実現する方法を示す。

【0076】基本的には本実施例の構成やチケットの生成方法、全体の処理の流れは実施例 1 と同様である。本実施例の全体の構成を図 16 に示す。本実施例の特徴として、内部状態の中に、回数券の残り度数を示すカウンタ 202a が設置されている点が異なる。図 16 においては、図 2 と対応する箇所に対応する符号を付した。

【0077】利用者は回数券を購入すると、はじめに証明装置 200 に登録する。登録時に回数券に対応する内部状態記憶領域が確保され、そのなかのカウンタ 202a に、残りの使用回数を書き込まれる。

【0078】回数券の利用時には利用者は、証明装置 200 に対してこれから利用するチケットとして、チケット指定装置 300 により、回数券を指定した上で、検証装置 100 と証明装置 200 との間で認証プロトコルが開始される。

【0079】認証プロトコルでは、検証装置 100 が、認証情報として乱数 C を生成し証明装置 200 に送り、証明装置 200 が、チケット秘密鍵を計算するところまでは、実施例 1 と同様である。

【0080】本実施例のチケット証明情報生成処理 (図 3 の S33 に対応) のフローチャートを図 17 に示す。図 17 において、証明装置 200 のチケット判定情報生成部 203 は、この回数券のチケットに対応した内部状態の残り回数を抽出し、チケット利用情報とともに、チケット判定情報 M に記録する (S81~S84)。そして、実施例 1 と同様に、証明情報生成部 206 がチケット証明情報 T を生成し (S85)、認証情報生成部 20

4 が第 2 の認証情報 x を生成する (S86)。T と x は通信部 208 により検証装置 100 に送られる (S34)。

【0081】T と x を受け取った検証装置 100 はチケット判定処理 (図 3 の S35 に対応) を行う。

【0082】チケット判定処理のフローチャートを図 18 に示す。図 18 において、検証装置 100 の証明情報検証部 104 は、受け取ったチケット証明情報を検証する (S91)。チケット証明情報が正しい場合には、チケット証明情報から、チケット判定情報 M を抽出する (S92)。チケット判定情報 M には回数券の残り回数が記録されている。チケット判定部 101 はその値が 1 以上であれば、この回数券はまだ使用可能であると判断する (S93)。さらに、チケット利用情報 L の内容も、この検証装置 100 で検証可能であるとチケット判定部 101 が判断した場合には、証明情報生成部 103 は証明装置 200 の内部状態の変更を指示する情報 μ を作成する (S94、S95)。μ の内容として、回数券の使用回数を 1 減らすことを指示する内容が含まれる。そして、実施例 1 と同様の方法で、μ を使用して第 2 の証明情報 ρ を作成し (S96、S97)、証明装置 200 へと送る (S36)。

【0083】検証やチケット判定に失敗したときにはエラー処理を行なう (S98)。

【0084】ρ を受け取った証明装置 200 は内部状態変更処理 (図 3 の S37 に対応) を行う。

【0085】内部状態変更処理のフローチャートを図 19 に示す。図 19 において、証明装置 200 の証明情報検証部 205 は送られた第 2 の証明情報 ρ を検証する (S101)。正しいものであることが確認できた場合には、内部状態制御部が μ の内容に応じて、回数券の残り使用回数を 1 減らし、その結果を M' とする (S102~S104)。あとは、実施例 1 と同様の方法で、証明装置 200 は証明情報 R を生成して、検証装置 100 に送る (S105、S106)。ステップ S101 で検証に失敗したときにはエラー処理が行なわれる (S107)。

【0086】以降の検証装置 100 の動作は、実施例 1 と同様であり、R の値を検証して、サービスの提供を行う。

【0087】【実施例 4】本発明の実施例 4 では、全体の構成は実施例 1 と同様であるが、チケット公開情報・チケット秘密情報やチケットの認証方法が異なる。

【0088】本実施例では、p が素数であり、G が離散対数問題が困難な有限群であり、g が有限群 G の位数 p の元であり、

【0089】

【数 14】 $y = g^x \pmod{p}$ が満たされるとき、(p, G, g, y) がチケット公開情報であり、x をチケット秘密情報とする。(p, G,

g) はシステム全体で共通とすることもできる。

【0090】このとき、チケットはチケット特徴情報 x と証明装置固有情報 du とチケット利用情報 L と、群を規定する情報 p より、

【0091】

【数15】 $t = x - F(du, L, y, p)$

として、計算される。ここで、 F は非衝突性の一方関数であり、一般のハッシュ関数によって実現可能である。 L は実施例 1 と同様のチケット利用情報である。

【0092】また、検証装置の特権をあらわすものとして、上記 (p, G, g) は共通として、

【0093】

【数16】

$$\eta = g^f \bmod p$$

を満たすような η を公開情報、 ϵ を秘密情報とする。

【0094】実際には G を乗法群として構成したり、有限体上の楕円曲線として構成することができる。

【0095】本発明の認証プロトコルの概略を図 20 に示す。

$$\begin{aligned} t + F(y, L, du, p) \\ = x - F(y, L, du, p) + F(y, L, du, p) \\ = x \end{aligned}$$

次に、チケット判定情報生成部 203 は、正しいチケットを保持していることを示すためのチケット判定情報 M を、チケットの付加情報 L や内部状態の情報から生成する (S212)。証明情報生成部 206 は、証明情報として、以下の値を生成する (S213、S214)。

【0101】

【数18】 $T = (C || M) \cdot C' \bmod p$

なお証明情報 T は上記以外にも、以下の式によっても計算できる。

【0102】

【数19】

$T = (C || M) \cdot C' C'^{r'} \bmod p$

また、認証情報生成部 204 は同時に乱数 r' を生成して、

【0103】

【数20】 $x = g^f \bmod p$

を第 2 の認証情報として検証装置に送る (S215、S216、S205)。チケット判定情報 M に入る情報は実施例 1 ～ 3 と同様である。

【0104】証明情報 T と第 2 の認証情報 x は、通信部 208 により検証装置 100 に送られる。

【0105】 T と x を受け取った検証装置 100 はチケット判定処理 (図 20 の S206) を行う。

【0106】チケット判定処理のフローチャートを図 22 に示す。図 22 において、検証装置 100 の証明情報検証部 103 は、送られたチケット証明情報から、

【0107】

【数21】 $T / y' \bmod p = (C || M) \cdot C' /$

【0096】はじめに利用者は、これから利用するチケットを証明装置に対して指定した上で、検証装置と証明装置の間で認証プロトコルが開始される。

【0097】図 20 において、この認証プロトコルでは、まず検証装置 100 の認証情報生成部 102 が、乱数 r を生成し、 $C = g^r$ を計算して、これを認証情報として証明装置に送る (S201、S202、S203)。

【0098】認証情報 C を受け取った証明装置 200 は、チケット証明情報生成処理を実行する (S204)。

【0099】チケット証明情報生成処理のフローチャートを図 21 に示す。図 21 において、まず証明装置 200 の証明情報生成部 206 は、署名に用いる秘密鍵 x を、チケット t とチケット利用情報 L 、チケット公開情報の p 、および証明装置固有情報 du から、以下の計算により算出する (S211)。

【0100】

【数17】

$$y' \bmod p$$

の値を計算し、そのビット列のうち、連結された M 以外の部分が、認証情報 C と一致するかどうかを確認する

(S221)。一致した場合には、チケット判定部 101 はさらにチケット判定情報 M の内容から、チケット及びチケットに関連付けられた内部状態がこの検証装置 100 で検証して良いものかどうかを判定する (S222、S223)。判定の結果、このチケットを検証して良い場合には、証明情報生成部 103 は証明装置 200 の内部状態の変更を指示する情報 μ を作成して、 x に連結する (S224、S225)。そして、この値に対して、検証装置の特権を表す秘密情報 ϵ を用いて以下の値を第 2 の認証情報として、生成する (S226)。

【0108】

【数22】

$$\rho = (x || \mu) \cdot x^f \bmod p$$

ρ は通信部 106 により証明装置 200 へと送られる。一方、チケット証明情報が正しいものでない場合や、チケットが検証すべきでないものの場合には、プロトコルを終了する (S227)。

【0109】次に ρ を受け取った証明装置 200 は内部状態変更処理 (図 20 の S208) を行う。

【0110】内部状態変更処理のフローチャートを図 23 に示す。図 23 において、証明装置 200 の証明情報検証部 205 は、送られた応答情報から、

【0111】

【数23】

$$\rho / \eta^{r'} \bmod p = (x || \mu) \cdot x^f / \eta^{r'} \bmod p$$

の値を計算し、そのビット列のうち、連結された μ 以外の部分が、第2の認証情報 x と一致するかどうかを確認する(S231)。正しいものであることが確認できた場合には、内部状態制御部207が、 μ の内部状態の変更を指示する情報に応じて、証明装置200の内部状態が変更し、その結果を M' とする(S232~S234)。一方、確認の結果、正しくないことが判明した場合には場合には、プロトコルを終了する(S137)。

【0112】証明情報生成部206は、 M' の値を認証情報Cのビット列に連結した上で、以下の値を証明情報として生成する(S235、S236)。

【0113】

$$[数24] R = (C || M') \cdot C' \bmod p$$

こうして生成された証明情報Rが通信部208により検証装置100に送られる(S209)。

【0114】Rを受け取った検証装置100は、証明情報検証処理S210(図2.0)を行う。

【0115】証明情報検証処理のフローチャートを図24に示す。図24において、証明情報検証部104は、送られたチケット証明情報から、

【0116】

$$[数25] R / y' \bmod p = (C || M') \cdot C' / y' \bmod p$$

の値を計算し、その結果 M' を除いた上位のビット列が、最初に検証装置100が生成した認証情報Cと一致することを確認する(S241)。確認できた場合は、さらに内部状態の変更結果を表す情報 M' の内容が、第2の証明情報 ρ として送った、内部状態変更を許可する情報 μ と一致するかどうかを確認し(S242、S243、S244)、確認ができた場合には、定められたサービスを提供する(S245)。いずれかの確認に失敗した場合には、プロトコルが終了し、サービスの提供は行われない(S246)。

【0117】

【発明の効果】以上で説明したように、本発明によれば、検証装置が検証可能なチケットのみを検証し、検証することが正しくないチケットに対しては、内部状態の変更を許可する情報を生成しないような電子チケットシステムを実現することができ、利用者の意図しない内部状態の変更や、内部状態の変更による不正行為を防止することができる。

【図面の簡単な説明】

【図1】 関連技術の処理を説明するフローチャートである。

【図2】 実施例1、2、4の構成を全体として示すブロック図である。

【図3】 実施例1の処理全体を説明するフローチャートである。

【図4】 実施例1の証明装置のチケット証明情報生成

処理を説明するフローチャートである。

【図5】 実施例1の検証装置のチケット判定処理を説明するフローチャートである。

【図6】 実施例1の証明装置の内部状態変更処理を説明するフローチャートである。

【図7】 実施例1の検証装置の証明情報検証処理を説明するフローチャートである。

【図8】 実施例2のトークンの初期の内部状態を示す図である。

【図9】 チケット付加情報の項目を示す図である。

【図10】 入場時にトークンから改札機に送られるチケット判定情報Mを示す図である。

【図11】 入場時に改札機からトークンに送られる項目 μ を示す図である。

【図12】 入場後のトークンの内部状態を示す図である。

【図13】 出場時にトークンから改札機に送られるチケット判定情報Mを示す図である。

【図14】 出場時に改札機からトークンに送られる情報 μ を示す図である。

【図15】 出場後のトークンの内部状態を示す図である。

【図16】 実施例3の構成を全体として示すブロック図である。

【図17】 実施例3の証明装置のチケット証明情報生成処理を説明するフローチャートである。

【図18】 実施例3の検証装置のチケット判定処理を説明するフローチャートである。

【図19】 実施例3の証明装置の内部状態変更処理を説明するフローチャートである。

【図20】 実施例4の処理を全体として示すフローチャートである。

【図21】 実施例4の証明装置のチケット証明情報生成処理を説明するフローチャートである。

【図22】 実施例4の検証装置のチケット判定処理を説明するフローチャートである。

【図23】 実施例4の証明装置の内部状態更新処理を説明するフローチャートである。

【図24】 実施例4の検証装置の証明情報検証処理を説明するフローチャートである。

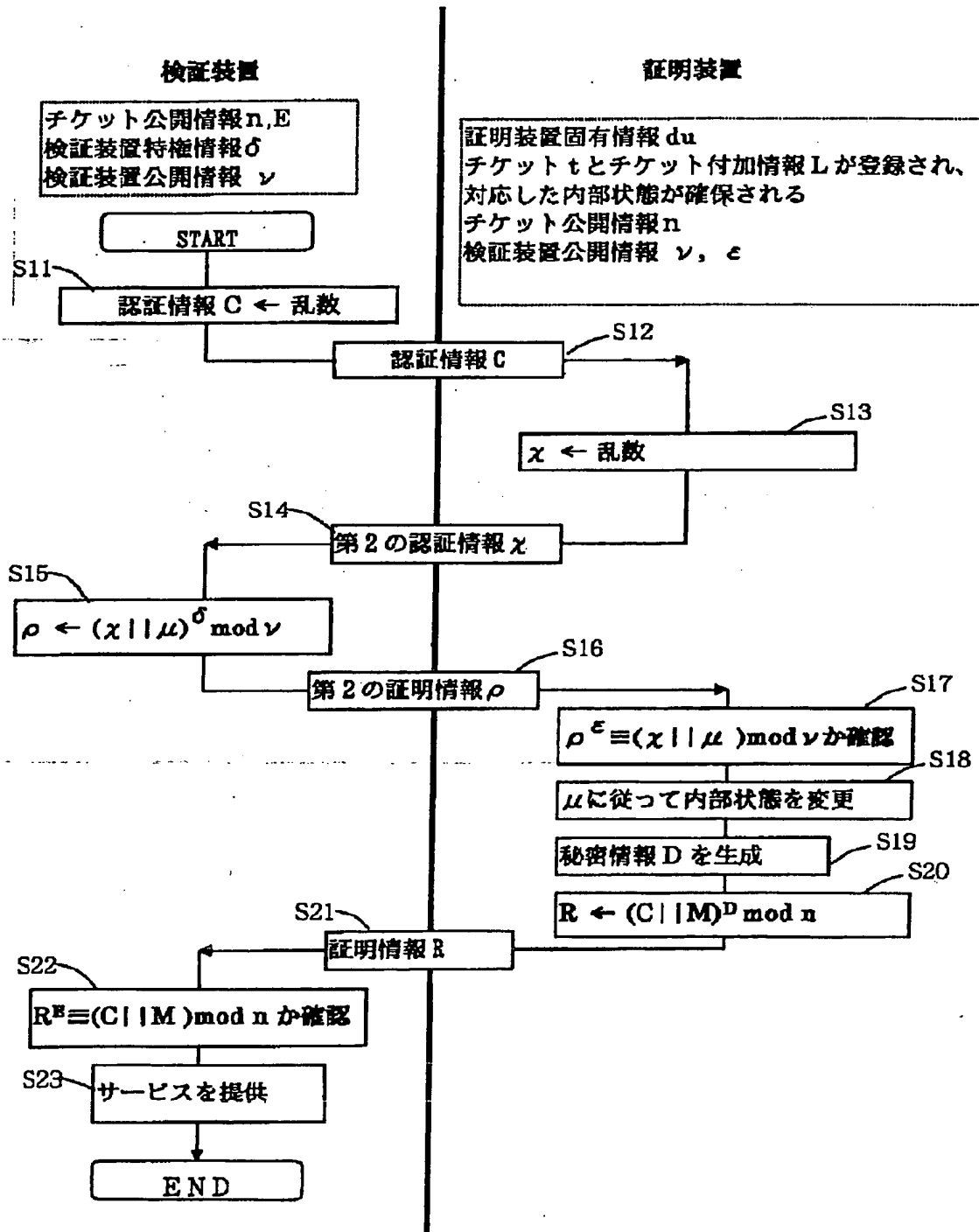
【符号の説明】

100	検証装置
101	チケット判定部
102	認証情報生成部
103	証明情報生成部
104	証明情報検証部
200	証明装置
201	証明装置固有情報保持部
202	チケット保持部

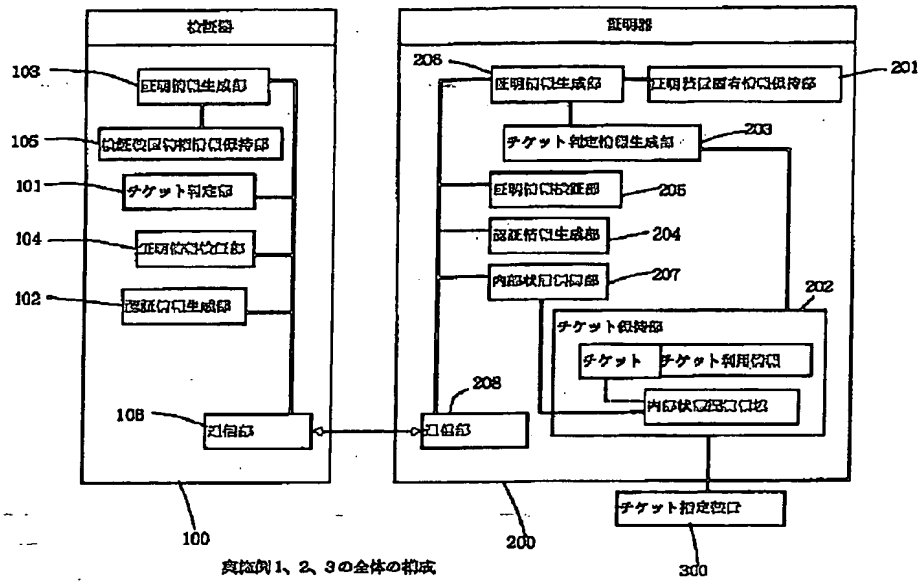
202a カウンタ
 203 チケット判定情報生成部
 204 認証情報生成部
 205 証明情報検証部

206 証明情報生成部
 207 内部状態制御部
 300 チケット指定装置

【図1】



【図 2】



【図 8】

【図 10】

入場時にトークンから読み込まれるチケット判定情報

出券所	目録	使用開始日	有効期限	入場	入場	出場	出場
横浜	成田空港	97/7/18	1日	東京	なし	なし	なし

トークン内の情報の内容

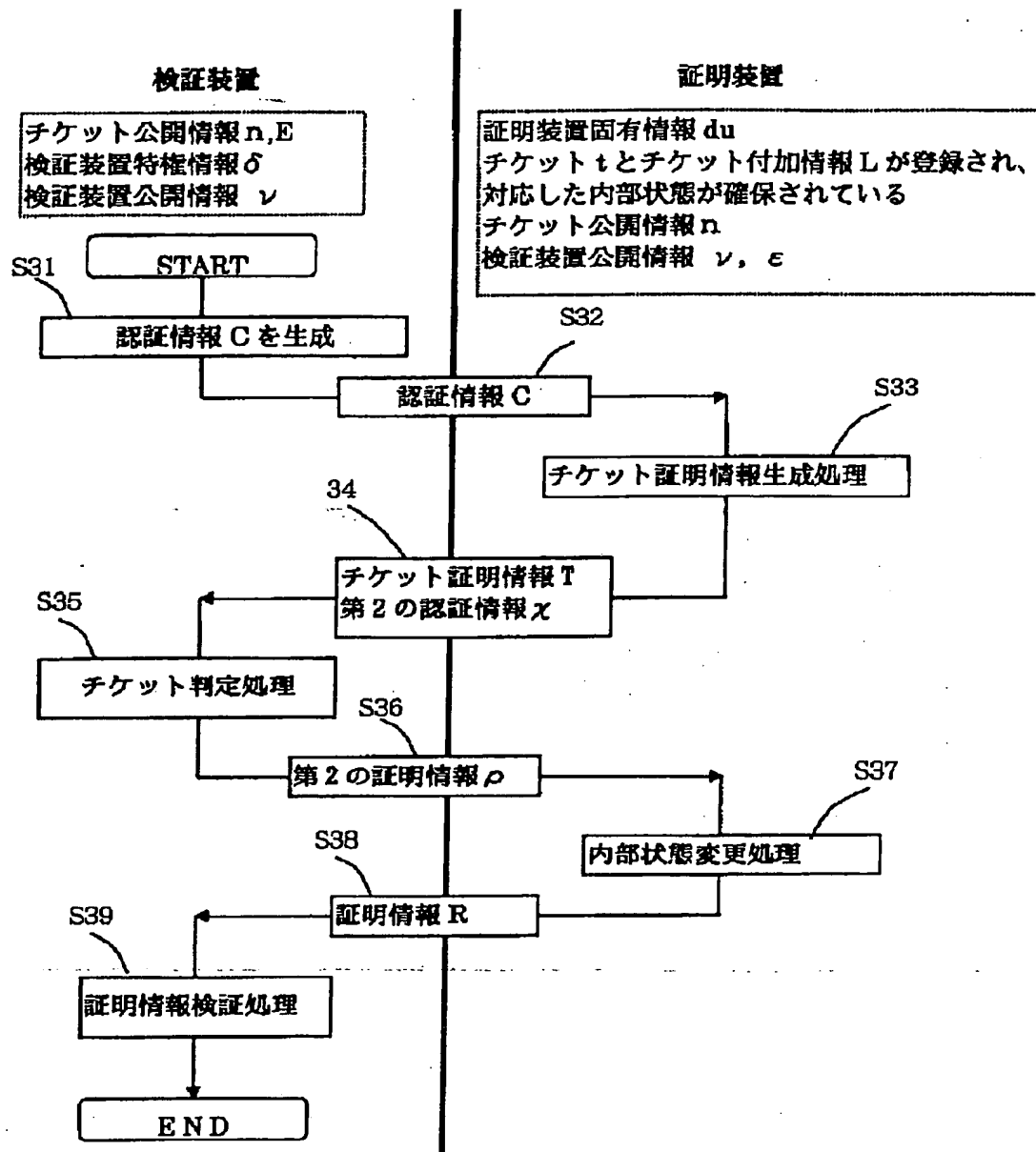
チケットID	発券所	現金形	目録	入場	出場	使用開始日	有効期限
00001	97/6/31	現金	なし	なし	なし	なし	なし
00003	97/6/31	クレジット	なし	97/6/31, 9:00	97/6/31, 9:30	なし	なし
00005	97/7/10	現金	なし	なし	なし	なし	なし

【図 9】

チケット利用情報の項目

発行ID	発券所	現金形	出券所	目録	発行日時	使用開始日	有効期限	座席
00123	平塚	現金	横浜	成田空港	97/7/10	97/7/18	1日	東京

【図 3】



実施例 1 の処理全体のフローチャート

【図 1 1】

入場時に改札機からトークンに渡される項目 μ (増設駅で入場)

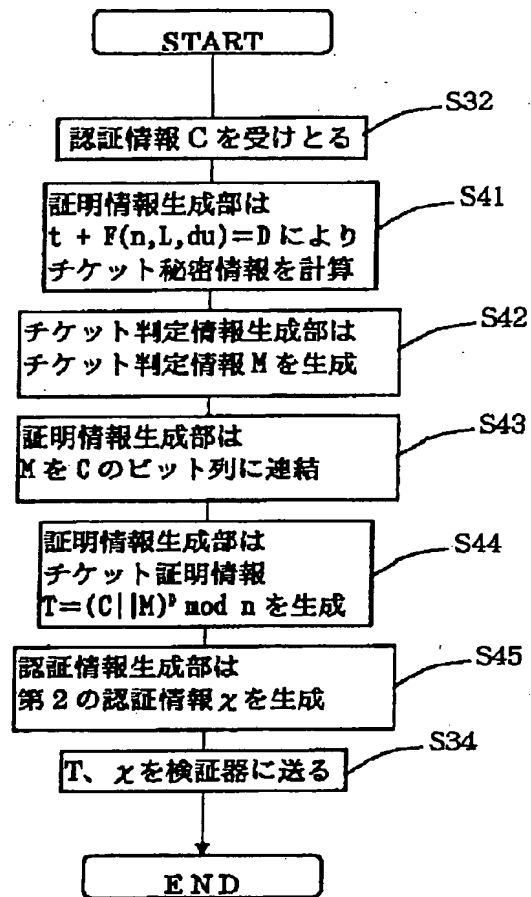
入場駅	入場時刻
横浜	97/7/18, 8:20

【図 1 2】

入場後のトークンの内部状態

チケット ID	発券情報	現金形態	変更記録	入場記録	出場記録	残札記録
00001	97/6/31	現金	なし	なし	なし	なし
00003	97/6/31	クレジット カード	なし	97/6/31, 8:05 横浜	97/6/31, 8:20 平塚	なし
00005	97/7/10	現金	なし	97/7/18, 6:20 横浜	なし	なし

【図 4】

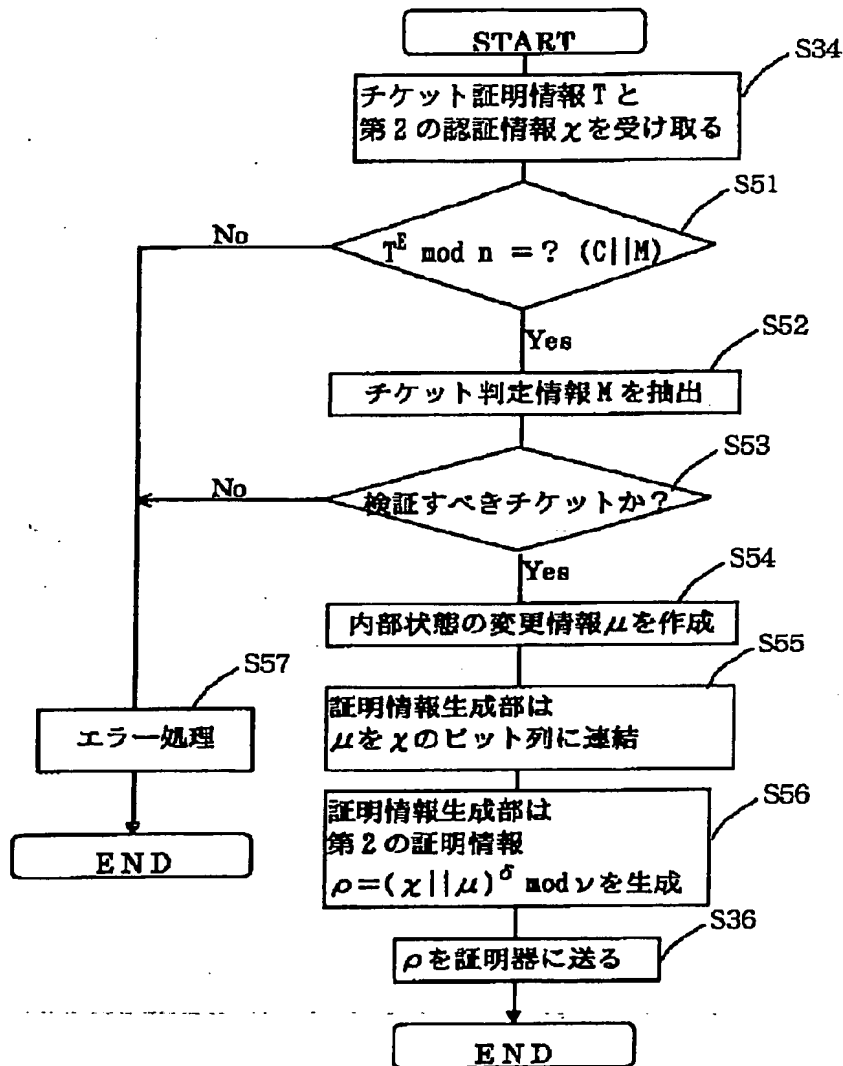
実施例 1 の証明装置のチケット証明情報生成処理のフローチャート

【図 13】

出場時にトークンから改札機に送られるチケット判定情報 M

出発駅	目的駅	使用開始日	有効期間	経路	入場記録	出場記録	検札記録
横浜	成田空港	97/7/18	1 日	東京	97/7/18, 6:20 横浜	なし	なし

【図 5】



実施例 1 の検証装置のチケット判定処理のフローチャート

【図 14】

出場駅	出場時間
成田空港	97/7/18, 8:53

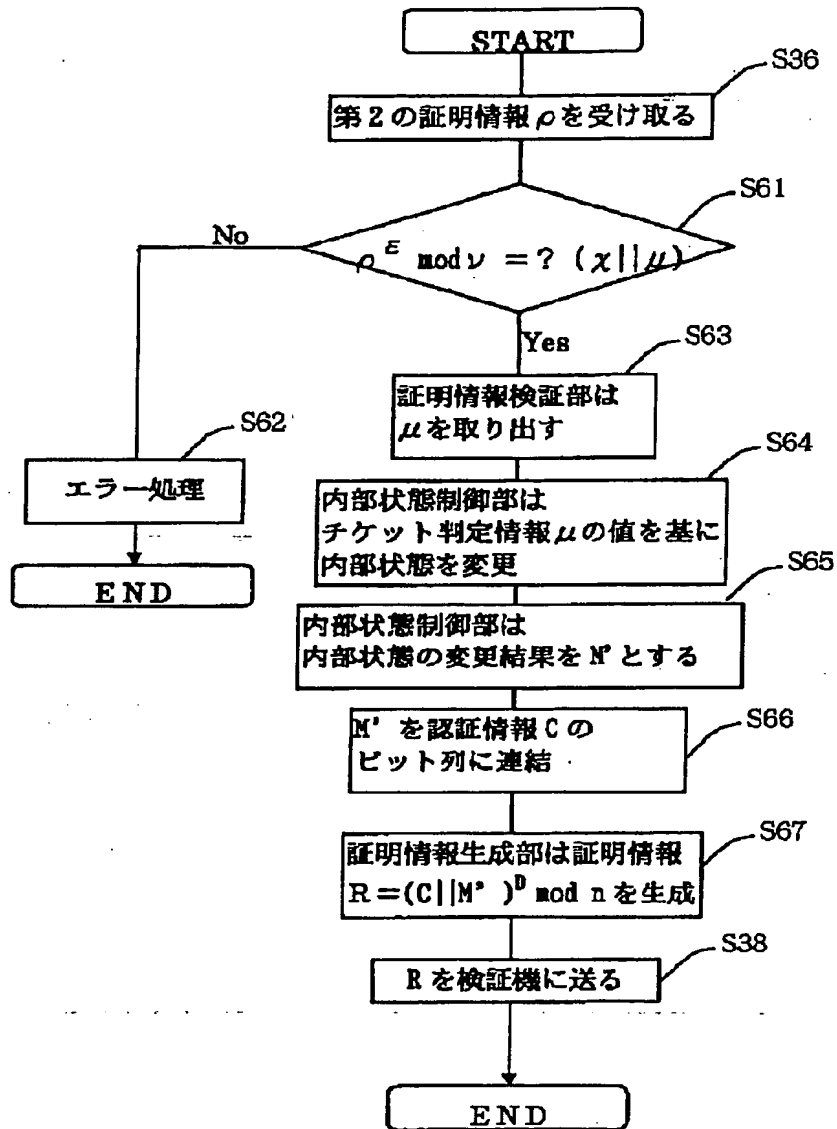
！出場時に改札機からトークンに送られる情報 μ (成田空港駅で出場)

【図 15】

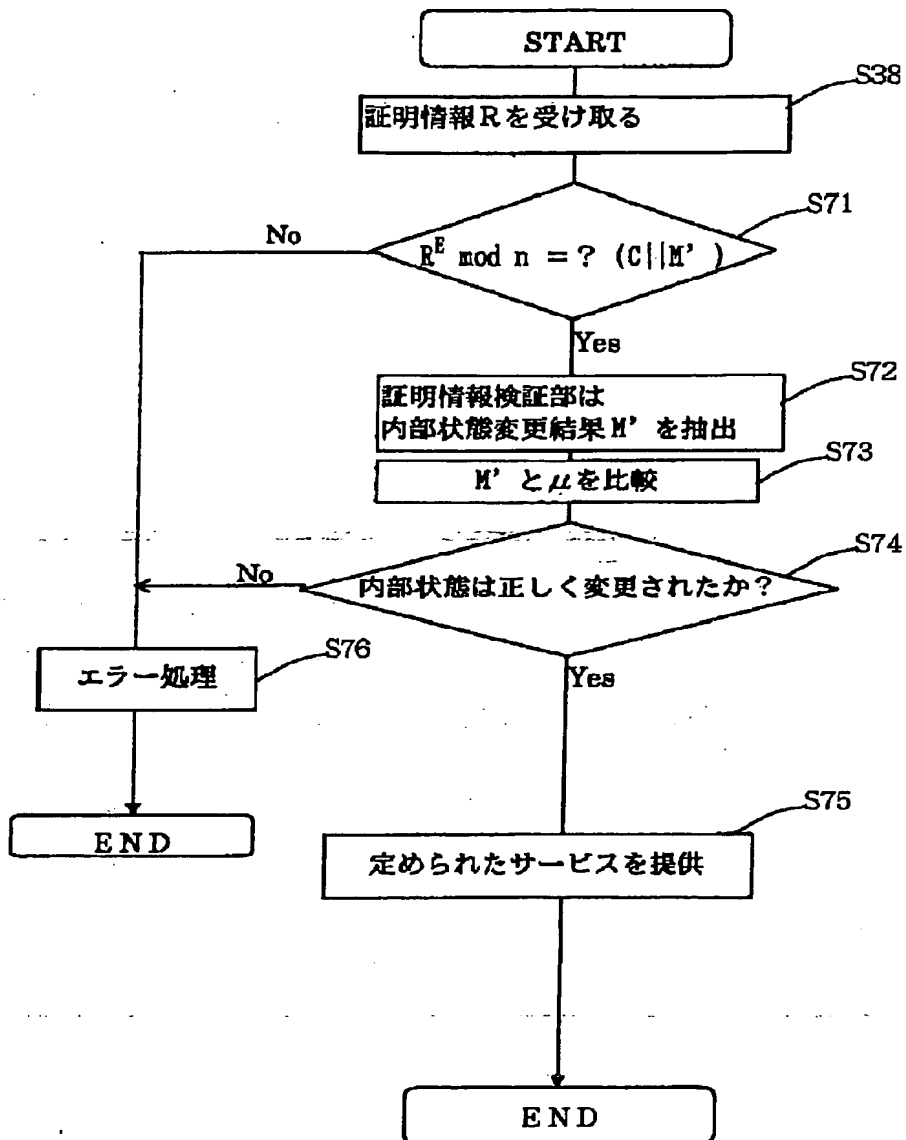
出場時のトークンの内部状態

チケット ID	発券情報	課金形態	変更記録	入場記録	出場記録	検札記録
00001	97/6/31	現金	なし	なし	なし	なし
00003	97/6/31	クレジット カード	なし	97/6/31, 9:05 横浜	97/6/31, 9:20 平塚	なし
00005	97/7/10	現金	なし	97/7/18, 6:20 横浜	97/7/18, 8:53 成田空港	なし

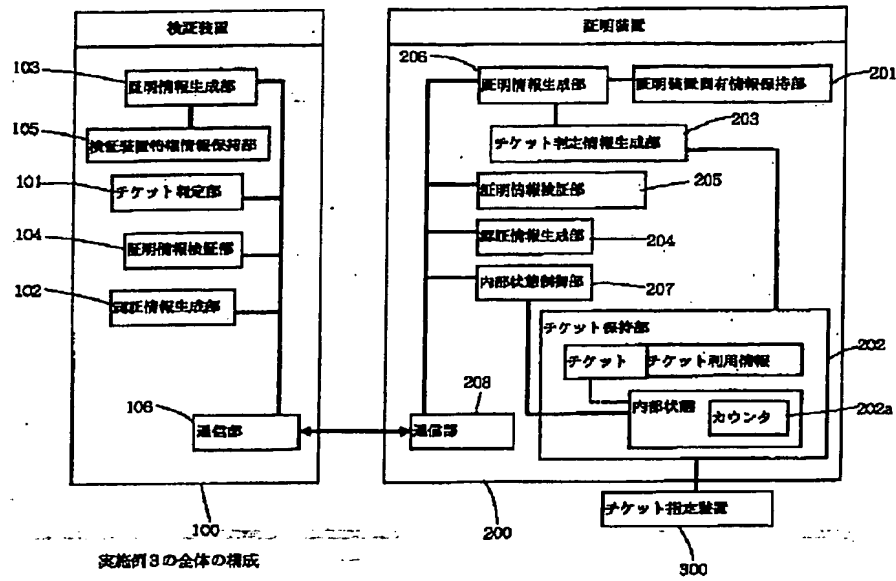
【図 6】

実施例 1 の証明装置の内部状態変更処理のフローチャート

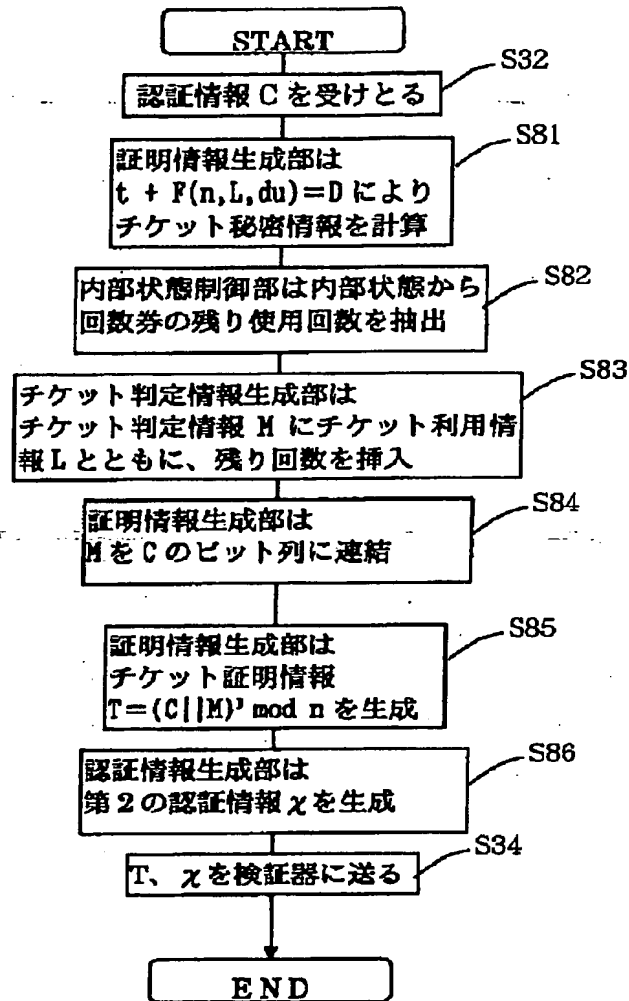
【図 7】

実施例 1 の検証装置の証明情報検証処理のフローチャート

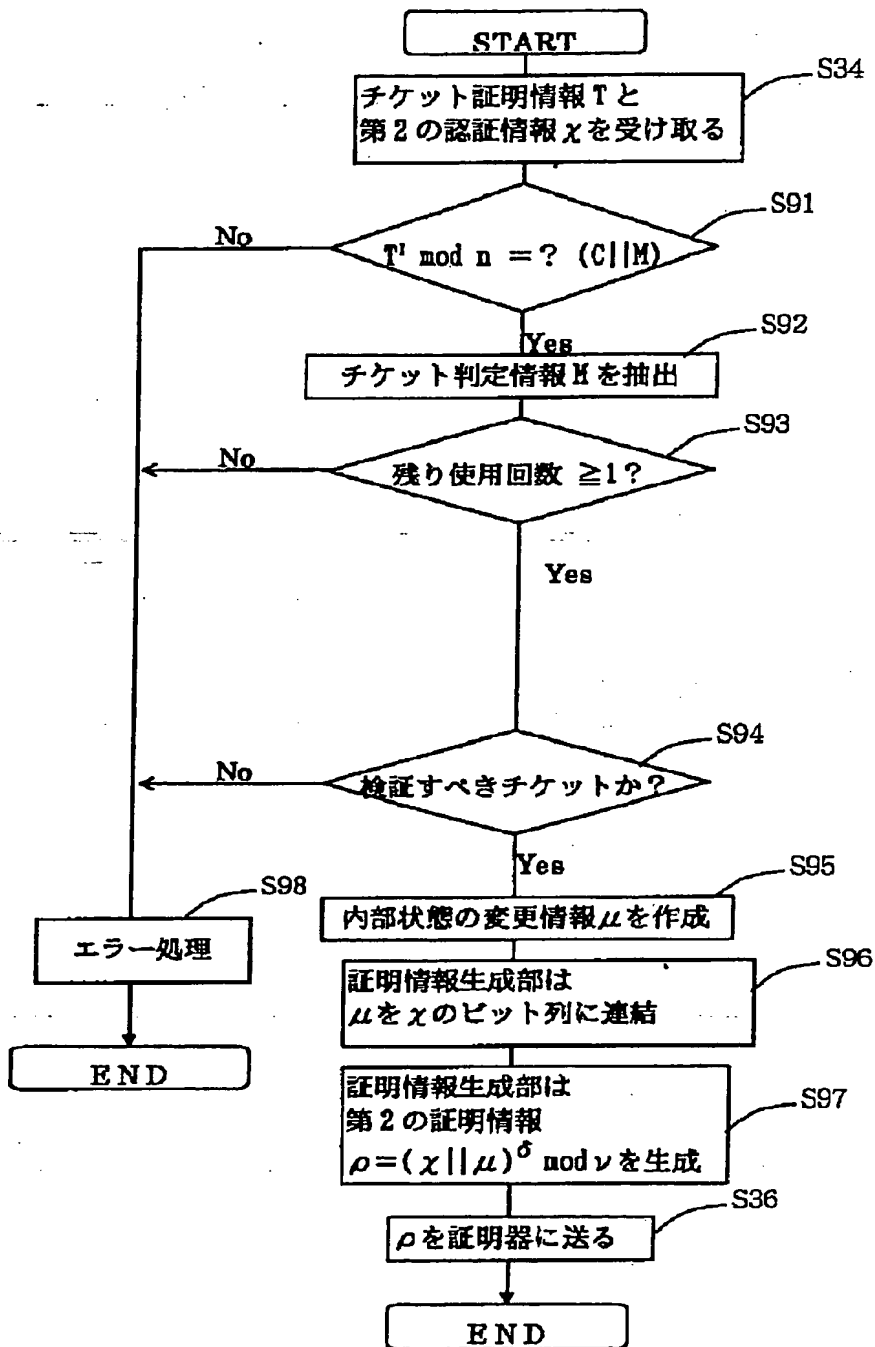
【図 1 6】



【図 17】

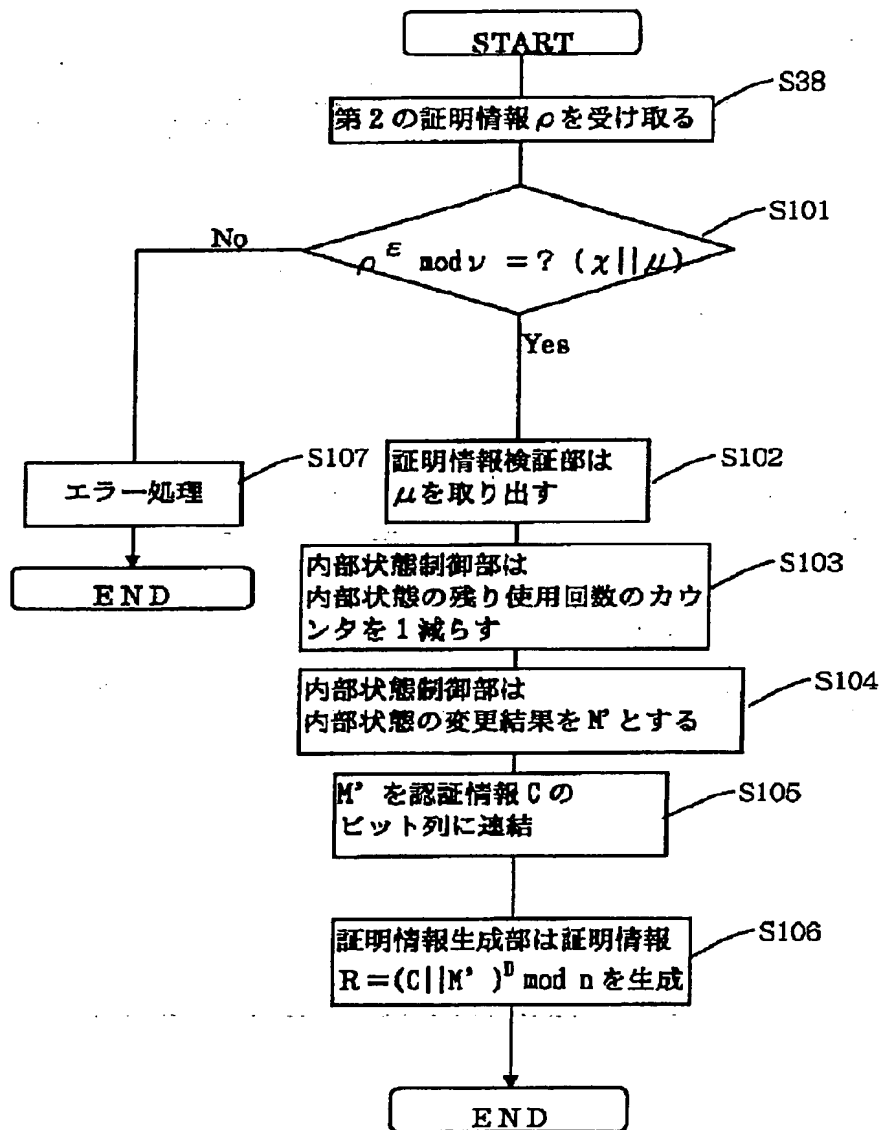
実施例 3 の証明装置のチケット証明情報生成処理のフローチャート

【図 18】

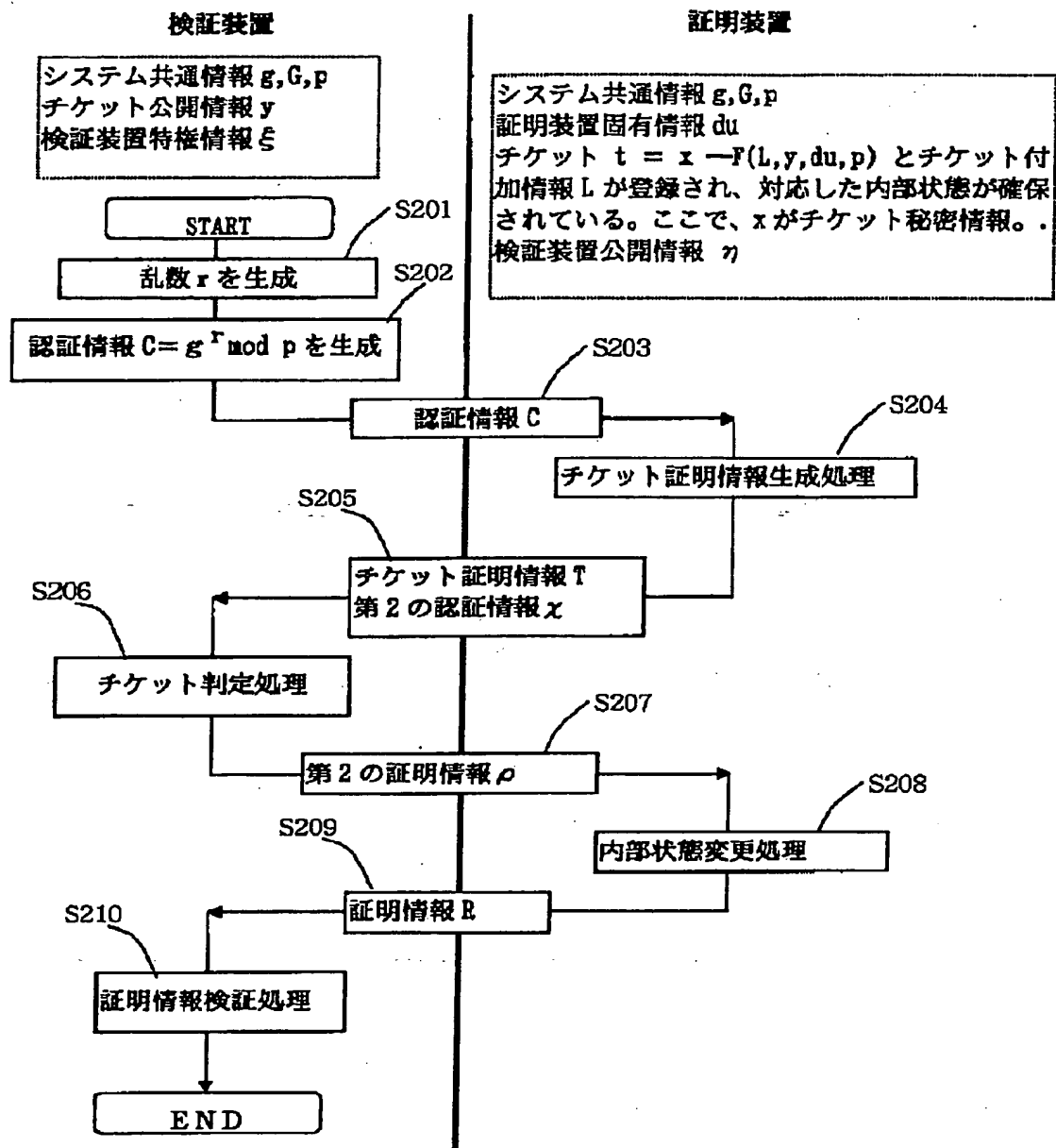


実施例 3 の検証装置のチケット判定処理のフローチャート

【図 19】

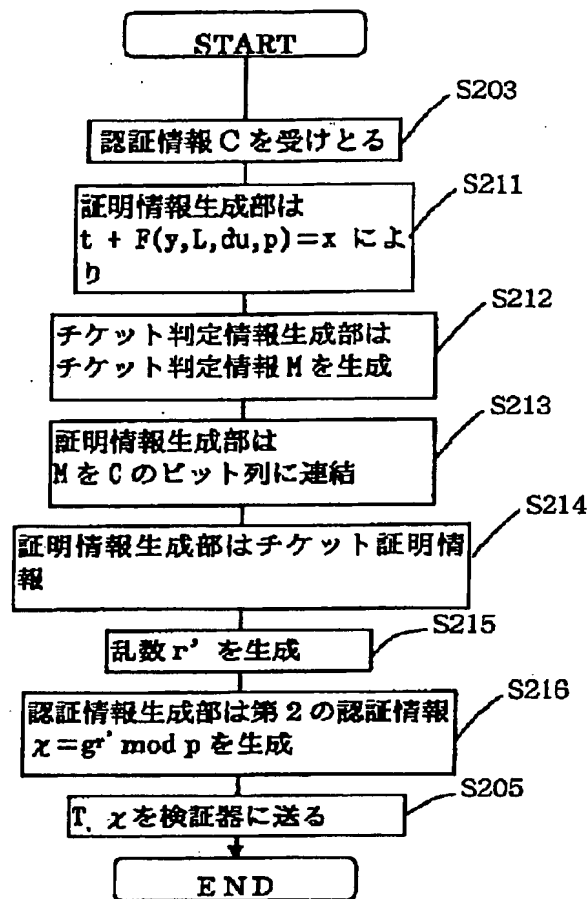
実施例3の証明装置の内部状態変更処理のフローチャート

【図 20】

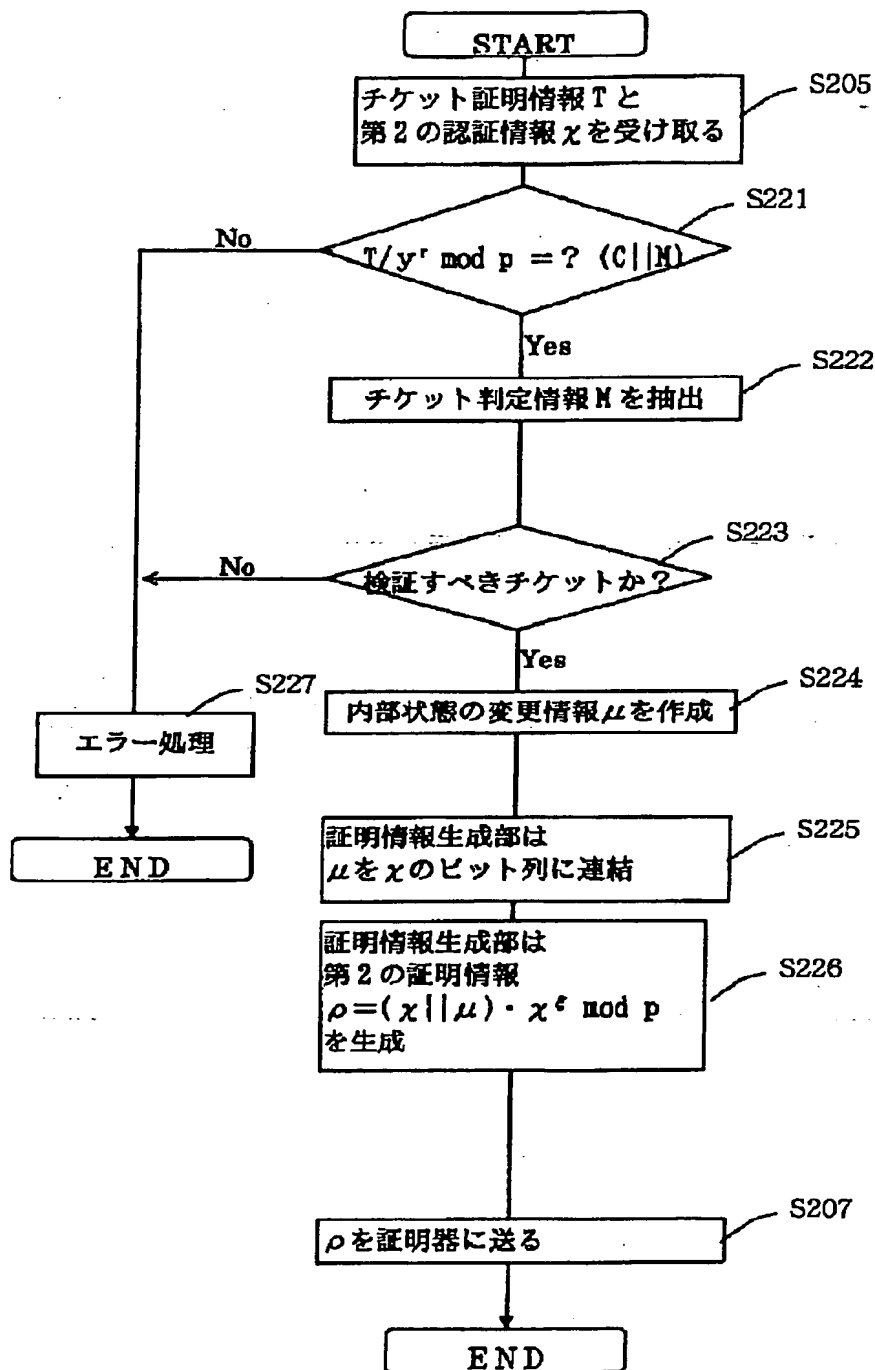


実施例 4 の処理全体のフローチャート

【図 21】

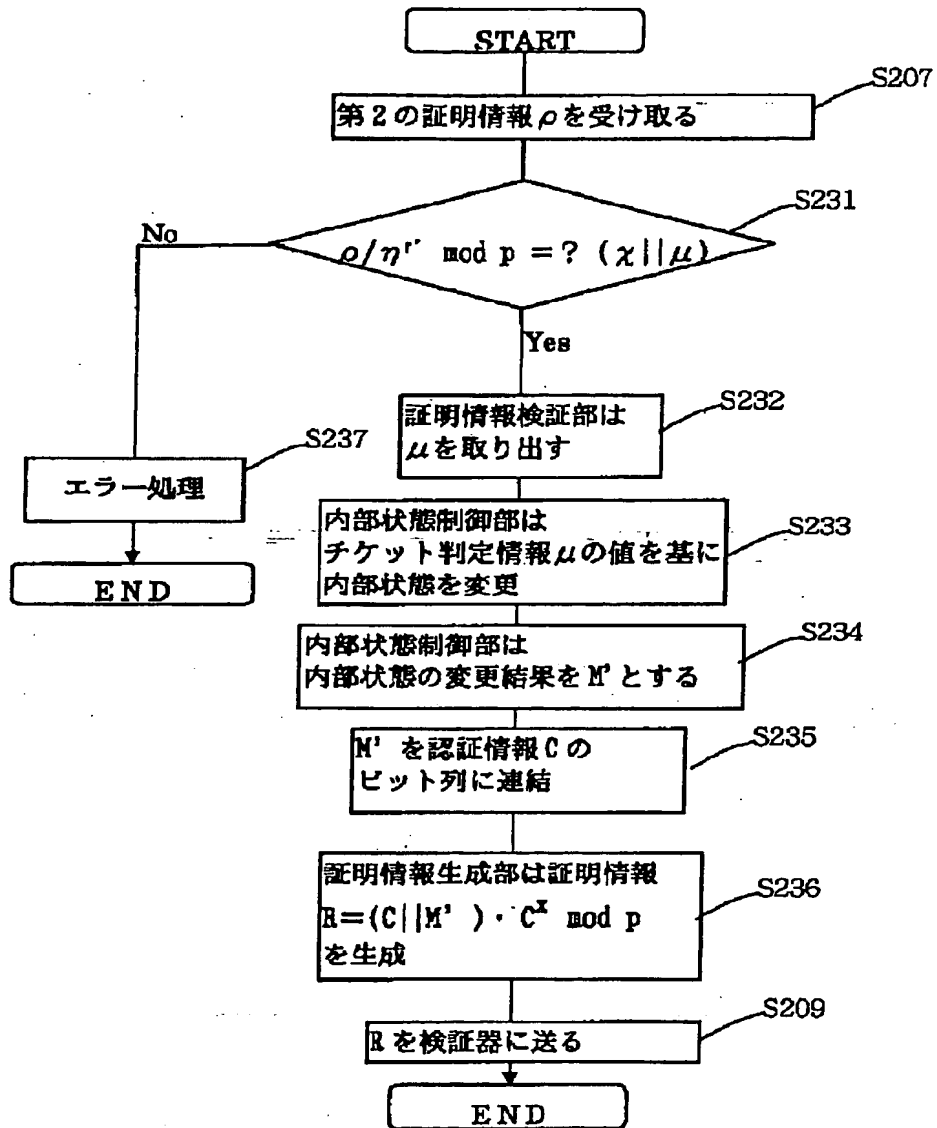
実施例 4 の証明装置のチケット証明情報生成処理のフローチャート

【図 2 2】



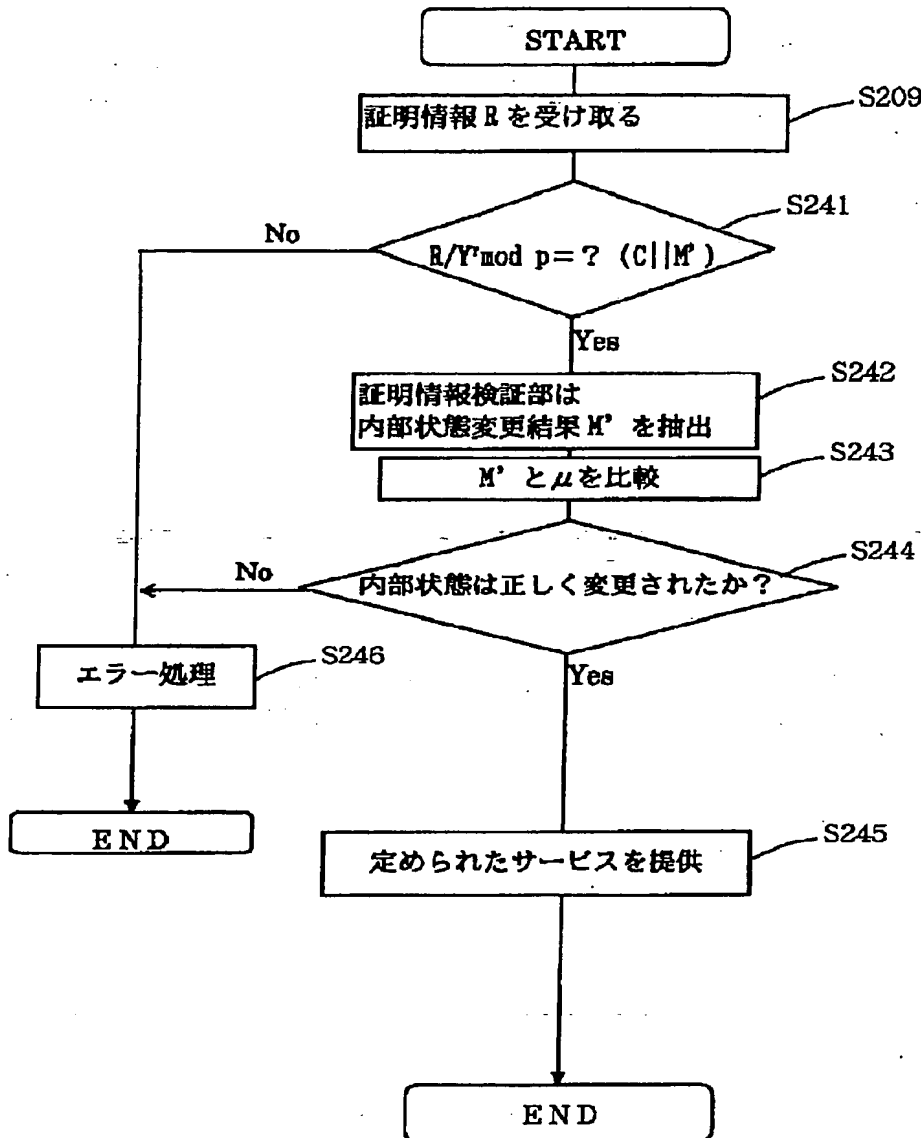
実施例 4 の検証装置のチケット判定処理のフローチャート

【図 23】



実施例4の証明装置の内部状態更新処理のフローチャート

【図 2 4】



実施例 4 の検証装置の証明情報検証処理のフローチャート

フロントページの続き

(51) Int. Cl.	識別記号	庁内整理番号	F I	技術表示箇所
			5/00	C
	5/00		G09C 1/00	Z
G07F 7/12			G06F 15/21	C
G09C 1/00	660		G07F 7/08	C
			H04L 9/00	Z
			660	
			340	
			675	

(72)発明者 谷口 慎一郎
神奈川県足柄上郡中井町境 4 3 0 グリー
ンテクノikai 富士ゼロックス株式会社内